



CVE-2020-5594

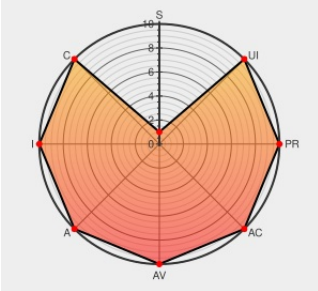
Published on: 06/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5594

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Melsec-fx](#) from [Mitsubishielectric](#) contain the following vulnerability:

Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors.

CVE-2020-5594 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Mitsubishi Electric Corporation](#) - MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules version **all versions**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Vendor Advisory	MISC
	www.mitsubishielectric.com	www.mitsubishielectric.com/en/bsirt/vulnerability/pdf/2020-

	www.mitsubishielectric.com/application/pdf	www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-003_en.pdf
JVNVU#91424496: Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series vulnerable to cleartext transmission of sensitive information	Third Party Advisory jvn.jp text/xml	MISC jvn.jp/en/vu/JVNVU91424496/index.html

	Vendor Advisory www.mitsubishielectric.co.jp application/pdf	MISC www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2020-003.pdf
--	--	--

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

590626 Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L and FX Series CPU Modules (Update A) Uncontrolled Resource Consumption Vulnerability (ICSA-20-175-01)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Mitsubishielectric	Melsec-fx	-	All	All	All
Hardware 	Mitsubishielectric	Melsec-fx	-	All	All	All
Operating System	Mitsubishielectric	Melsec-fx Firmware	All	All	All	All
Operating System	Mitsubishielectric	Melsec-fx Firmware	All	All	All	All
Hardware 	Mitsubishielectric	Melsec-l	-	All	All	All
Hardware 	Mitsubishielectric	Melsec-l	-	All	All	All
Operating System	Mitsubishielectric	Melsec-l Firmware	All	All	All	All
Operating System	Mitsubishielectric	Melsec-l Firmware	All	All	All	All
Hardware 	Mitsubishielectric	Melsec-q	-	All	All	All
Hardware 	Mitsubishielectric	Melsec-q	-	All	All	All
Operating System	Mitsubishielectric	Melsec-q Firmware	All	All	All	All
Operating System	Mitsubishielectric	Melsec-q Firmware	All	All	All	All
Hardware 	Mitsubishielectric	Melsec Iq-f	-	All	All	All
Hardware 	Mitsubishielectric	Melsec Iq-f	-	All	All	All
Operating System	Mitsubishielectric	Melsec Iq-f Firmware	All	All	All	All
Operating System	Mitsubishielectric	Melsec Iq-f Firmware	All	All	All	All

Hardware 	Mitsubishielectric	Melsec Iq-r	-	All	All	All
Hardware 	Mitsubishielectric	Melsec Iq-r	-	All	All	All
Operating System	Mitsubishielectric	Melsec Iq-r Firmware	All	All	All	All
Operating System	Mitsubishielectric	Melsec Iq-r Firmware	All	All	All	All
cpe:2.3:h:mitsubishielectric:melsec-fx:-:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec-fx:-:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec-fx_firmware:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec-fx_firmware:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec-l:-:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec-l:-:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec-l_firmware:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec-l_firmware:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec-q:-:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec-q:-:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec-q_firmware:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec-q_firmware:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec_iq-f:-:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec_iq-f:-:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec_iq-f_firmware:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec_iq-f_firmware:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec_iq-r:-:*:*:*:*:*:						
cpe:2.3:h:mitsubishielectric:melsec_iq-r:-:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec_iq-r_firmware:*:*:*:*:*:						
cpe:2.3:o:mitsubishielectric:melsec_iq-r_firmware:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)