Multiple vulnerabilities due to Intel products in multiple FA products (December 2023)

Release date December 7, 2023
Mitsubishi Electric Corporation

■Overview

Multiple vulnerabilities caused by Intel products exist in multiple Mitsubishi Electric FA products. These vulnerabilities may allow a malicious attacker to disclose information in the affected products.

■CVSS[1]

CVE-2022-21151	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N	Base Score: 5.3
CVE-2021-33149	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N	Base Score: 2.5

■Affected Products and Affected Vulnerabilities

The affected products and versions are as follows. For details on each vulnerability, please refer to Intel's advisory.

products	Module Name	versions	Applicable Vulnerability	Intel's Advisory
MELIPC series	MI5122-VW	All versions	CVE-2021-33149	INTEL-SA-00648
	MI2012-W	All versions	CVE-2022-21151 CVE-2021-33149	INTEL-SA-00617 INTEL-SA-00648
	MI1002-W	All versions	CVE-2021-33149	INTEL-SA-00648
	MI3321G-W	All versions	CVE-2022-21151 CVE-2021-33149	INTEL-SA-00617 INTEL-SA-00648
	MI3315G-W	All versions	CVE-2022-21151 CVE-2021-33149	INTEL-SA-00617 INTEL-SA-00648
MELSEC iQ-R series	R102WCPU-W	All versions	CVE-2021-33149	INTEL-SA-00648
MELSEC Q series	Q24DHCCPU-V	All versions	CVE-2021-33149	INTEL-SA-00648
	Q24DHCCPU-VG	All versions	CVE-2021-33149	INTEL-SA-00648
	Q24DHCCPU-LS	All versions	CVE-2021-33149	INTEL-SA-00648
	Q26DHCCPU-LS	All versions	CVE-2021-33149	INTEL-SA-00648

■Description

The following two vulnerabilities caused by Intel products exist in multiple Mitsubishi Electric FA products.

・CVE-2022-21151: A Information disclosure vulnerability due to Processor Optimization Removal or Modification of Security-critical Code (CWE-1037)[2]

・CVE-2021-33149: A Information disclosure vulnerability due to Observable Discrepancy (CWE-203)[3]

■Impact

These vulnerabilities may allow a malicious attacker to disclose information in the affected products.

■Countermeasures

Please carry out the following mitigations.

■Mitigation

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

– Restrict physical access to the product by unauthorized users.

■Contact information

Please contact your local Mitsubishi Electric representative.

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

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/1037.html
3 https://cwe.mitre.org/data/definitions/203.html