Vulnerabilities in ROBOGUIDE

Version 04
Issued Date : October 14, 2022
FANUC CORPORATION

Version	Date	Description
01	2022/04/08	The first edition registration
02	2022/04/27	Updated the description of Description
03	2022/06/29	Updated the description for attack complexity
04	2022/10/14	Added details to the attack complexity description

■Overview

Vulnerabilities have been reported for ROBOGUIDE. If these vulnerabilities are exploited by malicious attackers, the PC may not work correctly due to data corruption. The reported ROBOGUIDE vulnerabilities only occur if an attacker is able to gather knowledge about the environment in which ROBOGUIDE is operating. For example, a successful attack requires collecting details on the User's PC configuration settings, sequence numbers, or shared secrets. If you are using a product that is affected by these vulnerabilities, please take measures such as the workarounds described below. Security measures such as Firewall, Antivirus Protection, and Network Segmentation security controls for the entire system is recommended as part of preventative, detective, and response controls.

■Description

The reported vulnerabilities are shown below.

CVE-ID	Reference URL
CVE-2021-38483	https://nvd.nist.gov/vuln/detail/CVE-2021-38483
CVE-2021-43933	https://nvd.nist.gov/vuln/detail/CVE-2021-43933
CVE-2021-43986	https://nvd.nist.gov/vuln/detail/CVE-2021-43986
CVE-2021-43988	https://nvd.nist.gov/vuln/detail/CVE-2021-43988
CVE-2021-43990	https://nvd.nist.gov/vuln/detail/CVE-2021-43990

■Impact

If these vulnerabilities are exploited by malicious attackers, the PC may not work correctly.

■Affected products

ROBOGUIDE V9 Rev.T and earlier

■Countermeasures

Please consider executing 1 or 2 of the following measures.

- Countermeasure 1
  Please use ROBOGUIDE V9 Rev.U or higher.

- Countermeasure 2
  Make correct security settings such as anti-virus software and firewall on the PC.

We recommend that you take appropriate security measures for the entire system, not limited to the vulnerabilities described above.