Malicious Code Execution Vulnerability due to Flexera InstallShield Vulnerability in Multiple Software Tools and Industrial IoT-related Products for Mitsubishi Electric CNC Series

Release date: July 24, 2025
Mitsubishi Electric Corporation

Overview

Malicious code execution vulnerability due to DLL hijacking vulnerability caused by Flexera InstallShield exists in multiple software tools and industrial IoT-related products for Mitsubishi Electric CNC Series. A local attacker may be able to execute malicious code by getting setup-launcher to load a malicious DLL. (CVE-2016-2642)

Please note that this vulnerability only affects when the setup-launcher is run, not after installation.

CVSS[1]

CVE-2016-2542 CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H Base Score:7.0

Affected products

The affected products and versions are as follows.

Product name	Version
NC Designer2	All versions
NC Designer	All versions
NC Configurator2	All versions
NC Analyzer2	All versions
NC Analyzer	All versions
NC Explorer	All versions
NC Monitor2	All versions
NC Monitor	All versions
NC Trainer2 / NC Trainer2 plus	"AB" and prior
NC Trainer / NC Trainer plus	All versions
NC Visualizer	All versions
Remote Monitor Tool	All versions
MS Configurator	All versions
Mitsubishi Electric Numerical Control Device Communication Software (FCSB1224)	All versions
Mitsubishi Electric CNC communication software runtime library M70LC/M730LC	All versions
NC Virtual Simulator	All versions

<How to Check the Versions>
Please refer to the manual or help documentation for each product.
The manual can be downloaded from the following site.
https://www.mitsubishielectric.com/fa/download/index.html

Description

Malicious code execution vulnerability via DLL hijacking due to Uncontrolled Search Path Element (CWE-427[2]) exists in Flexera InstallShield used in multiple software tools and industrial IoT-related products for Mitsubishi Electric CNC Series.

Impact

A local attacker may be able to execute malicious code by getting setup-launcher to load a malicious DLL.

Countermeasures for Customers

- Customers using the affected products for which countermeasure versions are listed in "Countermeasures for Products".
  Please download and install the fixed version from the following site.
  https://www.mitsubishielectric.com/fa/download/index.html

- Customers using the affected products for which countermeasure versions are not listed in "Countermeasures for Products".
  Please take the following "Mitigations/Workarounds".

  Please note that there are no plans to release fixed versions for the following products:
  NC Designer

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/427.html

NC Analyzer
NC Monitor
NC Trainer / NC Trainer plus
NC Visualizer
Remote Monitor Tool
MS Configurator

Countermeasures for Products

The vulnerability is fixed in the following products and versions.

Product name	Version
NC Trainer2 / NC Trainer2 plus	"AC" or later

Mitigations / Workarounds

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

- Restrict physical access to the computer using the product.
- Install an antivirus software in the computer using the affected product.
- Do not open untrusted files or click untrusted links.
- Do not run setup-launchers obtained from sources other than our branches, distributors or the Mitsubishi Electric FA website.
- Before running the setup-launcher, make sure that no DLL exists in the folder containing the setup-launcher executable file (the name varies depending on the product) for the product.

Acknowledgement

Mitsubishi Electric would like to thank Sahil Shah who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.
<Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html