富士電機
Innovating Energy Technology

Document ID: PSA-HMI-2024-001
Published: June 3, 2024
Fuji Electric Co., Ltd.

Security Advisory: Multiple Vulnerabilities in V-SFT
(JVNVU#97725986)

1. Overview

Multiple vulnerabilities (3 in total) have been confirmed in the screen configuration software "V-SFT", which may lead to abnormal termination of the system, information disclosure, or arbitrary code execution. Customers are advised to review the details in this report and consider implementing the necessary actions.

2. Products Affected

Product Name (Model)	Affected Version
V-SFT	v6.2.3.0 and prior versions

3. Vulnerability Details

3.1 Contained Vulnerabilities

The product contains the following vulnerabilities:

(1)CVE-2024-5271

・Weakness: CWE-787 (Out-of-bounds Write)
・CVSS v4.0 Base Score: 8.5 (/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
・CVSS v3.1 Base Score: 7.8 (/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

(2)CVE-2024-34171

・Weakness: CWE-121 (Stack-based Buffer Overflow)
・CVSS v4.0 Base Score: 8.5 (/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
・CVSS v3.1 Base Score: 7.8 (/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

(3)CVE-2024-5597

・Weakness: CWE-843 (Type Confusion)
・CVSS v4.0 Base Score: 8.5 (/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
・CVSS v3.1 Base Score: 7.8 (/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

3.2 Impact

・Arbitrary code execution (CVE-2024-5271, CVE-2024-34171)
・Application crash or arbitrary code execution (CVE-2024-5597)

4. Remediation

Please update to the fixed version (V6.2.3.0 or later). The update modules and detailed release information are available via the support site of the manufacturer, Hakko Electronics Co., Ltd.

Please access the URL below and search by entering the Document Number:
URL: https://felib.fujielectric.co.jp/ja/document_search?region=jpn&tab=software
Document No.: "-"

5.Contact Information

Please contact our local branch offices or distributors where you purchased the product.

6. References

JVNVU#97725986: https://jvn.jp/vu/JVNVU97725986/
CVE-2024-5271: https://nvd.nist.gov/vuln/detail/cve-2024-5271
CVE-2024-34171: https://nvd.nist.gov/vuln/detail/cve-2024-34171
CVE-2024-5597: https://nvd.nist.gov/vuln/detail/cve-2024-5597

7. Update History

・June 3, 2024: First Edition