Document ID: PSA-HMI-2025-001
Published: May 14, 2025
Fuji Electric Co., Ltd.

Security Advisory: Multiple Vulnerabilities in V-SFT
(JVNVU#97228144)

1. Overview

Multiple vulnerabilities (12 in total) have been confirmed in the screen configuration software "V-SFT" provided by Fuji Electric Co., Ltd. If a user opens a specially crafted project file with an affected version of the product, it may lead to abnormal termination (denial of service), 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-6	v6.2.5.0 and prior versions

3. Vulnerability Details

3.1 Contained Vulnerabilities

The product contains the following vulnerabilities:

(1)CVE-2025-47749
- Weakness: CWE-761 (Free of Pointer not at the Beginning of Buffer)
- CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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-2025-47750
- Weakness: CWE-787 (Out-of-bounds Write)
- CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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-2025-47751
- Weakness: CWE-787 (Out-of-bounds Write)
- CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(4)CVE-2025-47752
- Weakness: CWE-787 (Out-of-bounds Write)
- CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(5)CVE-2025-47753
- Weakness: CWE-125 (Out-of-bounds Read)
- CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(6)CVE-2025-47754
- Weakness: CWE-125 (Out-of-bounds Read)
- CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(7)CVE-2025-47755
・Weakness: CWE-125 (Out-of-bounds Read)
・CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(8)CVE-2025-47756
・Weakness: CWE-125 (Out-of-bounds Read)
・CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(9)CVE-2025-47757
・Weakness: CWE-125 (Out-of-bounds Read)
・CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(10)CVE-2025-47758
・Weakness: CWE-121 (Stack-based Buffer Overflow)
・CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(11)CVE-2025-47759
・Weakness: CWE-121 (Stack-based Buffer Overflow)
・CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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)

(12)CVE-2025-47760
・Weakness: CWE-121 (Stack-based Buffer Overflow)
・CVSS v4.0 Base Score: 8.4 (/AV:L/AC:L/AT:N/PR:N/UI:A/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

Opening a specially crafted V-SFT file with the affected product may result in the following impacts:
・Abnormal termination of the system
・Information disclosure
・Execution of arbitrary code

4. Remediation

Please update to the fixed version (V6.2.6.0 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.: ”2504H25”

5. Acknowledgements

Fuji Electric extends its sincere gratitude to the following researcher for reporting these vulnerabilities under the Coordinated Vulnerability Disclosure (CVD) process:

Reporter: Michael Heinzl

6.Contact Information

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

7. References

JVNVU#97228144: https://jvn.jp/vu/JVNVU97228144/
CVE-2025-47749: https://www.cve.org/CVERecord?id=CVE-2025-47749
CVE-2025-47750: https://www.cve.org/CVERecord?id=CVE-2025-47750
CVE-2025-47751: https://www.cve.org/CVERecord?id=CVE-2025-47751
CVE-2025-47752: https://www.cve.org/CVERecord?id=CVE-2025-47752
CVE-2025-47753: https://www.cve.org/CVERecord?id=CVE-2025-47753
CVE-2025-47754: https://www.cve.org/CVERecord?id=CVE-2025-47754
CVE-2025-47755: https://www.cve.org/CVERecord?id=CVE-2025-47755
CVE-2025-47756: https://www.cve.org/CVERecord?id=CVE-2025-47756
CVE-2025-47757: https://www.cve.org/CVERecord?id=CVE-2025-47757
CVE-2025-47758: https://www.cve.org/CVERecord?id=CVE-2025-47758
CVE-2025-47759: https://www.cve.org/CVERecord?id=CVE-2025-47759
CVE-2025-47760: https://www.cve.org/CVERecord?id=CVE-2025-47760

8. Update History

・May 14, 2025: First Edition