Document ID: PSA-HMI-2025-002
Published: October 8, 2025
Fuji Electric Co., Ltd.

Security Advisory: Multiple Vulnerabilities in V-SFT
(JVNVU#90008453)

1. Overview

Multiple vulnerabilities (9 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	v6.2.7.0 and prior versions

3. Vulnerability Details

3.1 Contained Vulnerabilities

The product contains the following vulnerabilities:

(1)CVE-2025-61856
- 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)

(2)CVE-2025-61857
- 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-2025-61858
- 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-2025-61859
- 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-2025-61860
- 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-2025-61861
- 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-2025-61862
・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-2025-61863
・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-2025-61864
・Weakness: CWE-416 (Use After Free)
・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 project file with an affected version of V-SFT may result in the following impacts:

・Abnormal termination (ABEND) or denial-of-service (DoS) condition of the application/host system
・Unauthorized disclosure of sensitive data residing in memory
・Execution of arbitrary code in the context of the running process

4. Remediation

Please update to the fixed version (V6.2.8.0 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.: "25A0H08"

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#90008453 ： https://jvn.jp/vu/JVNVU90008453/
CVE-2025-61856 ： https://www.cve.org/CVERecord?id=CVE-2025-61856
CVE-2025-61857 ： https://www.cve.org/CVERecord?id=CVE-2025-61857
CVE-2025-61858 ： https://www.cve.org/CVERecord?id=CVE-2025-61858
CVE-2025-61859 ： https://www.cve.org/CVERecord?id=CVE-2025-61859
CVE-2025-61860 ： https://www.cve.org/CVERecord?id=CVE-2025-61860
CVE-2025-61861 ： https://www.cve.org/CVERecord?id=CVE-2025-61861
CVE-2025-61862 ： https://www.cve.org/CVERecord?id=CVE-2025-61862
CVE-2025-61863 ： https://www.cve.org/CVERecord?id=CVE-2025-61863
CVE-2025-61864 ： https://www.cve.org/CVERecord?id=CVE-2025-61864

8. Update History

・October 8, 2025: First Edition