Document ID: PSA-HMI-2024-003
Published: November 28, 2024
Fuji Electric Co., Ltd.

Security Advisory: Multiple Vulnerabilities in Multiple Products (JVNVU#97531313)

1. Overview

Multiple vulnerabilities (3 in total) have been confirmed in V-SFT, TELLUS, TELLUS Lite, V-Server, and V-Server Lite, which may result in 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

CVE	Product Name (Model)	Affected Version
CVE-2024-38309	V-SFT-6	v6.2.2.0 and prior versions
	TELLUS	v4.0.19.0 and prior versions
	TELLUS Lite	v4.0.19.0 and prior versions
CVE-2024-38389	TELLUS	v4.0.19.0 and prior versions
	TELLUS Lite	v4.0.19.0 and prior versions
CVE-2024-38658	V-Server	v4.0.19.0 and prior versions
	V-Server Lite	v4.0.19.0 and prior versions

3. Vulnerability Details

3.1 Contained Vulnerabilities

The following vulnerabilities exist in V-SFT, TELLUS, TELLUS Lite, V-Server, and V-Server Lite:

(1)CVE-2024-38309

・Weakness: CWE-121 (Stack-based Buffer Overflow)
・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-2024-38389

・Weakness: CWE-125 (Out-of-bounds Read)
・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-2024-38658

・Weakness: CWE-125 (Out-of-bounds Read)
・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 file may result in information disclosure or arbitrary code execution.

4. Remediation

Please update to the fixed version (V-SFT: V6.2.3.0 or later, TELLUS: V4.0.20.0 or later, V-Server: V4.0.20.0 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.: V-SFT:"-"
TELLUS:"2450Q01"
V-Server:"2450S03"

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#97531313: https://jvn.jp/vu/JVNVU97531313/
CVE-2024-38309: https://nvd.nist.gov/vuln/detail/cve-2024-38309
CVE-2024-38389: https://nvd.nist.gov/vuln/detail/cve-2024-38389
CVE-2024-38658: https://nvd.nist.gov/vuln/detail/cve-2024-38658

8. Update History

・November 28, 2024: First Edition