Document ID: PSA-HMI-2024-002
Published: June 14, 2024
Fuji Electric Co., Ltd.

Security Advisory: Multiple Vulnerabilities in Tellus Lite V-Simulator (JVNVU#96920775)

1. Overview

Multiple vulnerabilities (2 in total) have been confirmed in Tellus Lite V-Simulator, which may allow 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
Tellus Lite V-Simulator	v4.0.20.0 and prior versions

3. Vulnerability Details

3.1 Contained Vulnerabilities

The product contains the following vulnerabilities:

(1)CVE-2024-37022

・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:L/UI:N/S:U/C:H/I:H/A:H)

(2)CVE-2024-37029

・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:L/UI:N/S:U/C:H/I:H/A:H)

3.2 Impact

If these vulnerabilities are exploited, the affected product may suffer the following impact:

・Arbitrary code execution

4. Remediation

Please update to the fixed version (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.: "2450S03"

5.Contact Information

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

6. References

JVNVU#96920775: https://jvn.jp/vu/JVNVU96920775/
CVE-2024-37022: https://nvd.nist.gov/vuln/detail/cve-2024-37022
CVE-2024-37029: https://nvd.nist.gov/vuln/detail/cve-2024-37029

7. Update History

・June 14, 2024: First Edition