# SSA-543502: Local Privilege Escalation Vulnerability in Unicam FX

Publication Date: 2024-02-13
Last Update: 2024-02-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 8.5

## SUMMARY

Unicam FX contains a local privilege escalation vulnerability that could allow an attcker to gain SYSTEM privileges.

Unicam FX has reached end of software maintanence. Further information on recommendations for successor product can be found in section 'Additional Information'.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Unicam FX:<br>All versions<br>affected by all CVEs | Currently no fix is planned |

## WORKAROUNDS AND MITIGATIONS

Please follow the General Security Recommendations.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

## PRODUCT DESCRIPTION

UniCam FX provides a solution for standardizing PCB assembly process planning, machine programming and generating process documentation and hand insert instructions.

## VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### Vulnerability CVE-2024-22042

The windows installer agent used in affected product contains incorrect use of privileged APIs that trigger the Windows Console Host (conhost.exe) as a child process with SYSTEM privileges. This could be exploited by an attacker to perform a local privilege escalation attack.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C |
| CVSS v4.0 Base Score | 8.5 |
| CVSS Vector | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |
| CWE | CWE-648: Incorrect Use of Privileged APIs |

## ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Lockheed Martin Red Team for reporting the vulnerability

## ADDITIONAL INFORMATION

Unicam FX has reached end of software maintanence. In order to receive latest security and software updates, Siemens recommends to switch to the successor product Valor Process Preparation [1].

[1] https://plm.sw.siemens.com/en-US/valor/process-preparation/

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

## HISTORY DATA

V1.0 (2024-02-13): Publication Date

## TERMS OF USE