

## **SSA-829656: Stack Overflow Vulnerability in Xpedition Layout Browser**

Publication Date: 2023-10-10  
Last Update: 2023-10-10  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.8

### **SUMMARY**

Siemens Xpedition Layout Browser consists of a stack overflow vulnerability that could be triggered when the application reads a malicious file in PCB format. If a user is tricked to open a malicious file with the affected product, this could lead the application to crash or potentially lead to arbitrary code execution.

Siemens has released an update for Xpedition Layout Browser and recommends to update to the latest version.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
Xpedition Layout Browser: All versions < VX.2.14	Update to VX.2.14 or later version <a href="https://eda.sw.siemens.com/en-US/pcb/xpedition-enterprise/release-highlights-2-14/">https://eda.sw.siemens.com/en-US/pcb/xpedition-enterprise/release-highlights-2-14/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### **WORKAROUNDS AND MITIGATIONS**

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Do not open untrusted PCB files in Xpedition Layout Browser

Product-specific remediations or mitigations can be found in the section [Affected Products and Solution](#). 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**

Xpedition Layout Browser is a free tool to view and share of Xpedition PCB Layout Designs and schematic cross-probe to Xpedition.

## **VULNERABILITY CLASSIFICATION**

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (<https://www.first.org/cvss/>). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: <https://cwe.mitre.org/>.

### **Vulnerability CVE-2023-30900**

Affected application contains a stack overflow vulnerability when parsing a PCB file. An attacker can leverage this vulnerability to execute code in the context of the current process.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C</a>
CWE	CWE-121: Stack-based Buffer Overflow

## **ACKNOWLEDGMENTS**

Siemens thanks the following party for its efforts:

- Armando Guardasole from Telsy Elettronica e Telecomunicazioni for reporting the vulnerability

## **ADDITIONAL INFORMATION**

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 (2023-10-10): Publication Date

## **TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website ([https://www.siemens.com/terms\\_of\\_use](https://www.siemens.com/terms_of_use), hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.