SSA-988345: Local Privilege Escalation Vulnerability in Xpedition Designer

Publication Date: 2022-06-14
Last Update: 2023-06-13
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

SUMMARY

A vulnerability in Xpedition Designer could allow an attacker with an unprivileged account to override or modify the service executable and subsequently gain elevated privileges.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Xpedition Designer VX.2.10: All versions < VX.2.10 Update 13	Update to VX.2.10 Update 13 or later version https://support.sw.siemens.com/en-US/product/852852130/ See recommendations from section Workarounds and Mitigations
Xpedition Designer VX.2.11: All versions < VX.2.11 Update 11	Update to VX.2.11 Update 11 or later version https://support.sw.siemens.com/en-US/product/852852130/ See recommendations from section Workarounds and Mitigations
Xpedition Designer VX.2.12: All versions < VX.2.12 Update 5	Update to VX.2.12 Update 5 or later version https://support.sw.siemens.com/en-US/product/852852130/ See recommendations from section Workarounds and Mitigations
Xpedition Designer VX.2.13: All versions < VX.2.13 Update 1	Update to VX.2.13 Update 1 or later version https://support.sw.siemens.com/en-US/product/852852130/ See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Remove write permissions for every non-administrative user on files and folders located under the installation path
- Harden the application server to prevent local access by untrusted personnel

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 Enterprise is the industry's most innovative PCB design flow, providing integration from system design definition to manufacturing execution.

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-2022-31465

The affected application assigns improper access rights to the service executable. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.

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:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

ADDITIONAL INFORMATION

The previous update does not fully fix the vulnerability in versions prior or equal to VX.2.11. A new fix is then provided for VX.2.11 and also VX.2.10.

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 (2022-06-14):	Publication Date
V1.1 (2023-06-13):	Added new fix for versions VX.2.10 and VX.2.11. Added VX.2.12 and VX.2.13 as affected versions

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, 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.