SSA-439148: File Parsing Vulnerabilities in PADS Standard/Plus Viewer

Publication Date:	2022-07-12
Last Update:	2022-07-12
Current Version:	V1.0
CVSS v3.1 Base Score:	7.8

SUMMARY

Siemens PADS Standard/Plus Viewer is affected by multiple memory corruption vulnerabilities that could be triggered when the application reads files in PCB format. If a user is tricked to open a malicious file with the affected application, an attacker could leverage the vulnerability to perform remote code execution in the context of the current process

Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
PADS Standard/Plus Viewer: All versions	Currently no fix is planned 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:

- Do not open untrusted PCB files in PADS Standard/Plus Viewer

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

PADS Standard and Standard Plus provide PCB schematic design and layout capabilities in an intuitive and easy-to-use environment.

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-2022-34272

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-037, FG-VD-22-059)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34273

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-038)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-34274

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-039)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-34275

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-040)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-34276

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-041)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-34277

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-042)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34278

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-043)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34279

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-044)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34280

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-045)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34281

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to execute code in the context of the current process. (FG-VD-22-046)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34282

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-047)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34283

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-048)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34284

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-049)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-34285

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-050)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34286

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-051)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-34287

The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-052, FG-VD-22-056)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2022-34288

The affected application is vulnerable to an out of bounds read past the end of an allocated buffer when parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-053)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-34289

The affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted PCB files. This could allow an attacker to execute code in the context of the current process. (FG-VD-22-054)

CVSS v3.1 Base Score	7.8
CVSS Vector	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
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-34290

The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-055)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2022-34291

The affected application contains a stack corruption vulnerability while parsing PCB files. An attacker could leverage this vulnerability to leak information in the context of the current process. (FG-VD-22-057, FG-VD-22-058, FG-VD-22-060)

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Kushal Arvind Shah from FortiGuard Labs for coordinated disclosure of the vulnerabilities

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 (2022-07-12): 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, 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.