

Forum:[Hack Forums](#)

Thread: [Siemens Solid Edge](#)

Stanley - February 27, 2026, 2:05 pm

Siemens Solid Edge

View CSAF

Summary

Solid Edge uses PS/IGES Parasolid Translator Component that contains an out of bounds read that could be triggered when the application reads files in IGS file formats. If a user is tricked to open a malicious file with any of the affected products, this could lead the application to crash or potentially lead to arbitrary code execution. Siemens has released a new version for Solid Edge and recommends to update to the latest version.

The following versions of Siemens Solid Edge are affected:

Solid Edge: All versions prior to V226.00 Update 03

CVSS

Vendor

Equipment

Vulnerabilities

v3 7.8

Siemens

Siemens Solid Edge

Out-of-bounds Read

Background

Critical Infrastructure Sectors: Critical Manufacturing

Countries/Areas Deployed: Worldwide

Company Headquarters Location: Germany

Vulnerabilities

Expand All +

CVE-2025-40936

The affected applications contains an out of bounds read vulnerability while parsing specially crafted IGS files. This could allow an attacker to crash the application or execute code in the context of the current process. (ZDI-CAN-26755)

[View CVE Details](#)

Affected Products

Siemens Solid Edge

Vendor:Siemens

Product Version:Solid Edge

Product Status:known_affected

Remediations

Vendor fixUpdate to V226.00 Update 03 or later version

Relevant CWE: CWE-125 Out-of-bounds Read

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.1

7.8

HIGH

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Acknowledgments

Siemens ProductCERT reported this vulnerability to CISA.

Trend Micro Zero Day Initiative reported this vulnerability to Siemens.

General 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>

Additional Resources

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: <https://www.siemens.com/cert/advisories>

Terms of Use

The use of Siemens Security Advisories is subject to the terms and conditions listed on: <https://www.siemens.com/productcert/terms-of-use>.

Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

Recommended Practices

CISA recommends users take defensive measures to minimize the exploitation risk of these vulnerabilities.

Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolate them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most recent version available. Also recognize VPN is only as secure as its connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov](https://www.cisa.gov). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets. Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov](https://www.cisa.gov) in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

Advisory Conversion Disclaimer

This ICSA is a verbatim republication of Siemens ProductCERT SSA-445819 from a direct conversion of the vendor's Common Security Advisory Framework (CSAF) advisory. This is republished to CISA's website as a means of increasing visibility and is provided "as-is" for informational purposes only. CISA is not responsible for the editorial or technical accuracy of republished advisories and provides no warranties of any kind regarding any information contained within this advisory. Further, CISA does not endorse any commercial product or service. Please contact Siemens ProductCERT directly for any questions regarding this advisory.

Revision History

Initial Release Date: 2026-02-10

Date
Revision
Summary

2026-02-10

1

Publication Date

2026-02-12

2

Initial CISA Republication of Siemens ProductCERT SSA-445819 advisory

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-043-05>