

Forum:[Hack Forums](#)

Thread: [Siemens Desigo CC Product Family and SENTRON Powermanager](#)

Stanley - February 26, 2026, 7:55 am

Siemens Desigo CC Product Family and SENTRON Powermanager

View CSAF

Summary

Versions V6.0 through V8 QU1 of the Desigo CC product family (Desigo CC, Desigo CC Compact, Desigo CC Connect, Cerberus DMS), as well as the Desigo CC-based SENTRON Powermanager, are affected by a vulnerability in the underlying third-party component WIBU Systems CodeMeter Runtime. Successful exploitation of this vulnerability could lead to code execution in the context of the current process. Siemens has released instructions how to update the CodeMeter Runtime component and recommends to apply the update on affected systems.

The following versions of Siemens Desigo CC Product Family and SENTRON Powermanager are affected:

Desigo CC family V6 vers:all/* (CVE-2023-38545)

Desigo CC family V7 vers:all/* (CVE-2023-38545)

Desigo CC family V8: All versions prior to V8.0 QU2

SENTRON Powermanager V6 vers:all/* (CVE-2023-38545)

SENTRON Powermanager V7 vers:all/* (CVE-2023-38545)

SENTRON Powermanager V8: All versions prior to V8.0 QU2

CVSS

Vendor

Equipment

Vulnerabilities

v3 8.8

Siemens

Siemens Desigo CC Product Family and SENTRON Powermanager

Heap-based Buffer Overflow

Background

Critical Infrastructure Sectors: Critical Manufacturing

Countries/Areas Deployed: Worldwide

Company Headquarters Location: Germany

Vulnerabilities

Expand All +

CVE-2023-38545

This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake. When curl is asked to pass along the hostname to the SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that hostname can be is 255 bytes. If the hostname is detected to be longer than 255 bytes, curl switches to local name resolving and instead passes on the resolved address only to the proxy. Due to a bug, the local variable that means "let the host resolve the name" could get the wrong value during a slow SOCKS5 handshake, and contrary to the intention, copy the too long hostname to the target buffer instead of copying just the resolved address there.

[View CVE Details](#)

Affected Products

Siemens Desigo CC Product Family and SENTRON Powermanager

Vendor:Siemens

Product Version:Desigo CC family V6, Desigo CC family V7, Desigo CC family V8, SENTRON Powermanager V6, SENTRON Powermanager V7, SENTRON Powermanager V8

Product Status:known_affected

Remediations

Vendor fixUpdate to V8.0 QU2 or later version

Vendor fixUpdate to V8.0 QU2 or later version

Vendor fixApply patch as documented in section 'Additional Information'

Relevant CWE: CWE-122 Heap-based Buffer Overflow

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.1

8.8

HIGH

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

Acknowledgments

Siemens ProductCERT reported this vulnerability to CISA.

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-507364 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-507364 advisory

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-043-04>