Siemens Desigo Vulnerability Can Disrupt Building Automation Controllers

Author: *Portia S. Cole – CTI Researcher*

TL;DR

A medium-severity vulnerability (CVE-2026-59693, CVSS 4.3) affects several Siemens Desigo DXR and PXC building automation controllers.

An attacker with access to the building automation network can send a malformed BACnet packet that causes an affected controller to stop responding until it is reset or rebooted.

Overview

There is a medium-severity vulnerability (CVE-2026-59693, CVSS 4.3) in Siemens Desigo DXR and PXC controllers. The vulnerability is caused by improper handling of malformed BACnet packets.

An attacker does not need an account or user interaction to exploit the vulnerability. However, the attacker must be able to reach the controller from the same or an adjacent network.

Desigo controllers are used to manage HVAC and other building functions, such as lighting and room controls. Successful exploitation causes an affected controller to stop responding to BACnet queries. Facilities personnel must reset or reboot the controller to restore normal operation.

Affected Products

- Desigo DXR2 versions earlier than V01.21.233.16-7862
- Desigo PXC3 versions earlier than V01.21.233.16-7862
- Desigo PXC4 versions earlier than V02.21.194.36-2715
- Desigo PXC5.E003 versions earlier than V02.21.194.36-2715
- Desigo PXC5.E24 versions earlier than V02.21.194.36-2715
- Desigo PXC7 versions earlier than V02.21.194.36-2715

Siemens released updated versions for the affected products. The Siemens and Cybersecurity and Infrastructure Security Agency advisories do not report active exploitation.

Impact on Aspire Customers

For education customers, an unresponsive controller could lead to classroom temperature or ventilation problems. Indoor-air-quality monitoring and normal building schedules may also be affected until facilities staff restore the controller.

Other Aspire customers could experience similar building disruptions if affected controllers are used at their locations. The severity will depend on which systems each controller manages.

Aspire Protects

- **Patch** – Update Desigo DXR2 and PXC3 controllers to V01.21.233.16-7862 or later. See Siemens security advisory for further details.
- Update Desigo PXC4, PXC5.E003, PXC5.E24 and PXC7 controllers to V02.21.194.36-2715 or later.
- Prevent building automation controllers from being directly accessible from the internet.
- Place building automation systems behind firewalls and separate them from business networks.
- Restrict BACnet communications to approved systems and network segments.
- Monitor for unusual BACnet traffic and controllers that unexpectedly stop responding.

TTPs to Watch

Impact

- Denial of Service [T0814] – An attacker may send a malformed BACnet packet that causes an affected controller to stop responding to BACnet queries until the device is reset or rebooted.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This vulnerability could affect organizations in any industry that use the vulnerable controllers, including the following Aspire customer markets:

- Public Sector
- Energy
- Legal & Professional Services
- Healthcare
- Finance
- Education
- Retail
- Manufacturing

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

SSA-781903

Siemens Desigo DXR and PXC Controllers | CISA

NVD - cve-2026-59693