

Schneider Electric Security Notification

ASCO 5310 / 5350 Remote Annunciator

11 February 2025

Overview

Schneider Electric is aware of multiple vulnerabilities in its ASCO 5310 Remote Annunciator and ASCO 5350 Remote Annunciator products.

The [ASCO 5310 Remote Annunciator](#) and [ASCO 5350 Remote Annunciator](#) products are stand-alone, industrial grade interface devices providing transfer switch status indication and transfer/retransfer control.

Failure to apply the mitigations provided below may risk a Denial of Service, loss of availability, or loss of device integrity, which could result in the inability to use the Remote Annunciator to monitor transfer switch status and/or perform transfer/retransfer operations. The base operation of the transfer switch itself is not impacted.

Affected Products and Versions

Product	Version
ASCO 5310 Single-Channel Remote Annunciator	All Versions
ASCO 5350 Eight Channel Remote Annunciator	All Versions

Vulnerability Details

CVE ID: **CVE-2025-1058**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CVSS v4.0 Base Score 7.2 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-494: Download of Code Without Integrity Check vulnerability exists that could render the device inoperable when malicious firmware is downloaded.

CVE ID: **CVE-2025-1059**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-770: Allocation of Resources Without Limits or Throttling vulnerability exists that could cause communications to stop when malicious packets are sent to the webserver of the device.

CVE ID: **CVE-2025-1060**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Schneider Electric Security Notification

CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists that could result in the exposure of data when network traffic is being sniffed by an attacker.

CVE ID: **CVE-2025-1070**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CVSS v4.0 Base Score 7.2 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists that could render the device inoperable when a malicious file is downloaded.

The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 ([CVSS v4.0](#)). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Mitigations

Affected Product & Version	Mitigations
ASCO 5310 Single-Channel Remote Annunciator <i>All Versions</i>	<p>Schneider Electric is establishing a remediation plan for all future versions of ASCO 5310 Single-Channel Remote Annunciator and ASCO 5350 Eight Channel Remote Annunciator that may include a fix for these vulnerabilities. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none">• Use remote annunciator devices only in a protected environment to minimize network exposure and ensure that they are not accessible from public internet or untrusted networks.• Change default password to help prevent unauthorized access to device settings and information.• Setup network segmentation and implement a firewall to block all unauthorized access to the annunciator port 80/HTTP.• For more details on the ASCO 5310 refer to "Installation Manual ASCO 5310 ATS Remote Annunciator" which can be found here: https://www.se.com/ww/en/product-range/66129-asco-5310-singlechannel-remote-annunciator/-documents• For more details on the ASCO 5350 refer to "Installation Manual ASCO 5350 ATS Remote Annunciator" which can be found here: https://www.se.com/ww/en/product-range/66130-asco-5350-eight-channel-remote-annunciator/-documents
ASCO 5350 Eight Channel Remote Annunciator <i>All Versions</i>	

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here:

Schneider Electric Security Notification

<https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp>

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric [Recommended Cybersecurity Best Practices](#) document.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services:

<https://www.se.com/ww/en/work/solutions/cybersecurity/>. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric’s products, visit the company’s cybersecurity support portal page: <https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS “NOTIFICATION”) ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN “AS-IS” BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES

Schneider Electric Security Notification

WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.

www.se.com

Revision Control:

Version 1.0.0 11 February 2025	Original Release
--	-------------------------