

Schneider Electric Security Notification

Multiple Altivar Process Drives and Communication Modules

09 September 2025 (12 May 2026)

Overview

Schneider Electric is aware of a vulnerability in its [ATVdPAC module](#) / [ATV6000 Medium Voltage Altivar Process Drives](#) / [ATV630/650/660/680/6A0/6B0/6L0 Altivar Process Drives](#) / [ATV930/950/955/960/980/9A0/9B0/9L0 Altivar Process Drives](#) / [ATV340E Altivar Machine Drives](#) / [ATS490 Altivar Soft Starter](#) / [Altivar Process Communication Modules](#) product(s).

Failure to apply remediation/mitigations provided below may risk Cross-Site Scripting, which could result in partial loss of confidentiality and integrity of the workstation running a Web browser.

May 2026 Update: Remediations are now available for ATV6000 Medium Voltage Altivar Process Drives .

Affected Products and Versions

Product	Version
ATV630/650/660/680/6A0/6B0/6L0 Altivar Process Drives	Versions prior to v4.5
ATV930/950/955/960/980/9A0/9B0/9L0/991/992/993 Altivar Process Drives	Versions prior to v4.5
ILC992 InterLink Converter	All versions
ATV340E Altivar Machine Drives	Versions prior to v4.5
ATV6000 Medium Voltage Altivar Process Drives	Versions prior to v2.2
ATS490 Altivar Soft Starter	Versions prior to v1.2ie05
VW3A3720 & VW3A3721 Altivar Process Communication Modules	All versions
VW3A3530D: ATVdPAC module	Versions prior to v25.0

Vulnerability Details

CVE ID: **CVE-2025-7746**

CVSS v3.1 Base Score 6.1 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Base Score 5.3 | Medium | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause an unvalidated data injected by a malicious user potentially leading to modify or read data in a victim's browser.

Schneider Electric Security Notification

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.

Remediation

Affected Product & Version	Remediation
VW3A3530D: ATVdPAC module <i>Versions prior to v25.0</i>	Version 25.0 of VW3A3530D: ATVdPAC module includes a fix for this vulnerability and is available upon request from Schneider Electric's Customer Care Center .
ATV630/650/660/680/6A0/6B0/6L0 Altivar Process Drives <i>Versions prior to v4.5</i>	The version 4.5 of ATV6xx drives includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/62317-altivar-process-atv600/#software-and-firmware
ATV930/950/955/960/980/9A0/9B0/9L0/991/992/993 Altivar Process Drives <i>Versions prior to v4.5</i>	The version 4.5 of ATV9xx drives includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/63124-altivar-process-atv900/#software-and-firmware
ATV340E Altivar Machine Drives <i>Versions prior to v4.5</i>	The version 4.5 of ATV340E drives includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/63441-altivar-machine-atv340/#software-and-firmware
ATS490 Altivar Soft Starter <i>Versions prior to v1.2ie05</i>	The version 1.2ie05 of ATS490 drives includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/download/document/ATS490-Firmware/
ATV6000 Altivar Process Drives <i>Versions prior to v2.2</i>	Version 2.2 of ATV6000 drives includes a fix for this vulnerability and is available upon request from Schneider Electric's Customer Care Center .

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's [Customer Care Center](#) if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Schneider Electric Security Notification

Mitigations

Affected Product & Version	Mitigations
VW3A3530D: ATVdPAC module <i>Versions prior to v25.0</i> ATV630/650/660/680/6A0/6B0 Altivar Process Drives <i>Versions prior to v4.5</i> ATV930/950/955/960/980/9A0/9B0/9L0/991/992/993 Altivar Process Drives <i>Versions prior to v4.5</i> ATV340E Altivar Machine Drives <i>Versions prior to v4.5</i> ATS490 Altivar Soft Starter <i>Versions prior to v1.2ie05</i> ATV6000 Medium Voltage Altivar Process Drives <i>Versions prior to v2.2</i> ILC992 InterLink Converter VW3A3720 & VW3A3721 Altivar Process Communication Modules <i>All versions</i>	<p>Schneider Electric is establishing a remediation plan for all future versions of</p> <ul style="list-style-type: none"> • ILC992 InterLink Converter • VW3A3720 & VW3A3721 Altivar Process Communication Modules <p>that will include a fix for this vulnerability. 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"> • End user cybersecurity awareness and workstation protections • Deactivate the Webserver after use when not needed. • Setup network segmentation and implement a firewall to block all unauthorized access to port 80/HTTP • Use VPN (Virtual Private Networks) tunnels if remote access is required

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:

<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.

Schneider Electric Security Notification

- 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.

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2025-7746	Thomas Weber and David Blagojevic (CyberDanube)

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 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.

Schneider Electric Security Notification

About Schneider Electric

Schneider's purpose is to **create Impact** by empowering 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 the trusted partner in **Sustainability and Efficiency**.

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers**.

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Revision Control:

Version 1.0.0 09 September 2025	Original Release
Version 2.0.0 14 October 2025	Remediations are now available for ATV630/650/660/680/6A0/6B0/6L0 Altivar Process Drives, ATV930/950/955/960/980/9A0/9B0/9L0/991/992/993 Altivar Process Drives and ATV340E Altivar Machine Drives
Version 3.0.0 09 December 2025	Remediations are now available for ATS490 Altivar Soft Starter
Version 4.0.0 12 May 2026	Remediations are now available for ATV6000 Altivar Process Drives