

Schneider Electric Security Notification

Galaxy VS, Galaxy VL, Galaxy VXL

13 May 2025 (09 September 2025)

Overview

Schneider Electric is aware of a vulnerability disclosed on the Erlang/OTP's SSH Server component used Schneider Electric Galaxy VS, VL, and VXL.

Many vendors, including Schneider Electric, embed the Erlang/OTP's SSH Server in their offers.

The [Galaxy VS](#), [Galaxy VL](#), [Galaxy VXL](#) products are 3-phase UPS for data centers and other business critical applications.

Failure to apply the mitigation provided below may risk unauthenticated remote code execution (RCE), which could impact the monitoring capabilities of the UPS and potential UPS operation.

September 2025 Update: Remediations are now available for Galaxy VS, Galaxy VL, and Galaxy VXL.

Affected Products and Versions

Product	Version
Galaxy VS	v6.118.0 and prior
Galaxy VL	v18.5.0 and prior
Galaxy VXL	v15.21.0 and prior

Vulnerability Details

A vulnerability disclosed by Erlang/OTP's SSH Server impacts SSH component used on the Schneider Electric Galaxy VS, Galaxy VL, Galaxy VXL.

CVE ID: **CVE-2025-32433**

Additional information about the vulnerability CVE-2025-32433 can be found in the <https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgg5-7wc2>.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
Galaxy VS <i>v6.118.0 and prior</i>	Version 6.123.0 of Galaxy VS includes a fix for this vulnerability and is available through your local FSR by contacting Schneider Electric's Customer Care Center .
Galaxy VL <i>v18.5.0 and prior</i>	Version 18.10.0 of Galaxy VL includes a fix for this vulnerability and is available through your local FSR by contacting Schneider Electric's Customer Care Center .
Galaxy VXL <i>v15.21.0 and prior</i>	Version 15.29.0 of Galaxy VXL includes a fix for this vulnerability and is available through your local FSR by contacting Schneider Electric's Customer Care Center .

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/securitynotifications.jsp>

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

1. Log on to the NMC4 via the Web Interface. Once logged into the system, navigate to the Console settings page from the menu bar by selecting Configuration -> Network -> Console -> Access
2. From the Console setting screen, uncheck the enable SSH/SFTP/SCP check box -> Click Apply

As an alternative, setup network segmentation and implement a firewall to block all unauthorized access to SSH port 22/TCP.

If assistance is needed applying the above mitigation, please contact our technical support team: <https://www.se.com/ww/en/work/support/>

To learn more, we recommend reviewing the Network Management Card 4 Security Handbook for specific actions available here to secure your devices further: https://www.se.com/us/en/download/document/SPD_CCON-B8EJSJ_EN/

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>

Schneider Electric Security Notification

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

13-May-25 (09-Sep-2025) Document Reference Number – SEVD-2025-133-05 (v2.0.0) Page 3 of 4

Public / TLP: Clear

Schneider Electric Security Notification

“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.

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 13 May 2025	Original Release
Version 2.0.0 09 September 2025	Remediations are now available for Galaxy VS, Galaxy VL, and Galaxy VXL.