

NicheStack TCP/IP Vulnerabilities (INFRA:HALT) in Lexium ILE, ILA, ILS, and Communication Option Boards for Altivar and Lexium32 drives

05 August 2021 (09 May 2023)

Overview

Schneider Electric is aware of multiple vulnerabilities in HCC Embedded's NicheStack TCP/IP third party component, which is integrated into Schneider Electric's [Lexium ILE, ILA, ILS, Altivar Profinet Communication Module](#) (VW3A3627), (VW3A3616), and [Altivar 61/71 Profinet - Communication Card](#) (VW3A3327) products.

Failure to apply the mitigations provided below may risk denial of service of the drives.

May 2023 Update: A remediation is available for Altivar 32/320 & Lexium 32 Ethernet TCP/IP communication module (VW3A3616) ([page 2](#)).

Affected Products and Versions

Product	Version
Lexium ILE ILA ILS communication drive	Firmware communication module versions prior to V01.111
Altivar 32/320/340/600/900/6000 Profinet communication module (VW3A3627)	Firmware versions prior to V1.16IE01
Altivar 32/320 and Lexium 32 Ethernet TCP/IP communication module (VW3A3616)	Firmware versions prior to V1.20IE01
Altivar 61/71 Profinet communication card (VW3A3327)	All versions

Vulnerability Details

Five of the 14 vulnerabilities disclosed by researchers in the NicheStack TCP/IP component impact Schneider Electric's Lexium ILE, ILA, ILS, Altivar Profinet Communication Module (VW3A3627), Altivar and Lexium Ethernet TCP/IP Communication Module (VW3A3616), and Altivar Profinet - Communication Card (VW3A3327). Additional information about vulnerability details can be found at <https://us-cert.cisa.gov/ics/advisories/icsa-21-217-01>.

- [CVE-2021-31400](#)
- [CVE-2021-31401](#)
- [CVE-2020-35683](#)

- [CVE-2020-35684](#)
- [CVE-2020-35685](#)

Remediations

Affected Product & Version	Remediation /Mitigation
Lexium ILE ILA ILS Communication Drive <i>Versions prior to V01.111</i>	<p>V01.111 of Lexium ILE, ILA, ILS communication module includes a fix for these vulnerabilities.</p> <p>Reboot is needed.</p> <p>Please contact your local Schneider Electric technical support for more information on how to get the firmware and how to upgrade the communication firmware module.</p>
Altivar 32/320/340/600/900 Profinet communication module (VW3A3627) <i>Versions prior to V1.16IE01</i>	<p>V1.16IE01 of Altivar 32/320/340/600/900 Profinet communication module includes a fix for these vulnerabilities.</p> <p>For product release prior to V1.16IE01, apply the mitigations detailed in the Mitigations section and contact your local technical support for more information.</p>
Altivar 32/320 and Lexium 32 Ethernet TCP/IP communication module (VW3A3616) <i>Versions prior to V1.20IE01</i>	<p>V1.20IE01 of Altivar 32/320 and Lexium 32 Ethernet TCP/IP communication module includes a fix for these vulnerabilities.</p> <p>For product release prior to V1.20IE01, apply the mitigations detailed in the Mitigations section and contact your local technical support for more information.</p>
Altivar 61/71 Profinet communication card (VW3A3327) <i>All versions</i>	<p>This is an End Of Commercialization offer that is replaced by the ALTIVAR 900 & ALTIVAR 600 ranges.</p> <p>To reduce risk of exploitation, apply the mitigations detailed in the Mitigations section.</p>

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:

Mitigations

- Implement a firewall to restrict network access to the drives.
- Configure the controller associated to the drives by disabling IP forwarding as described in the online help of your controller.
- Configure the controller with dedicated access control lists as described below.

More information to implement these mitigations can be found in the online help of the controllers at:

https://olh.schneider-electric.com/Machine_Expert/V2.0/LandingPages/en/index.html

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 for the devices that it is intended for.
- 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 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 05 August 2021	Original Release
--------------------------------------	------------------

<p>Version 2.0 08 February 2022</p>	<p>Added <i>Altivar Profinet Communication Module (VW3A3627)</i>, <i>Lexium Ethernet TCP/IP Communication Module (VW3A3616)</i>, and <i>Altivar Profinet - Communication Card (VW3A3327)</i> to the list of affected products.</p>
<p>Version 3.0 13 September 2022</p>	<p>A remediation is available for Lexium ILE, ILA, ILS drives and the affected communication module firmware version has been updated.</p>
<p>Version 4.0 14 February 2023</p>	<p>A remediation is available for Altivar 32/320/340/600/900 Profinet communication module (VW3A3627) (page 2).</p>
<p>Version 5.0 09 May 2023</p>	<p>A remediation is available for Altivar 32/320 & Lexium 32 Ethernet TCP/IP communication module (VW3A3616) (page 2).</p>