

Schneider Electric Security Notification

Apache Log4j Vulnerabilities (Log4Shell)

13 December 2021 (11 October 2022)

Overview

Schneider Electric is aware of the vulnerabilities impacting Apache Log4j, including [CVE-2021-44228](#), also known as Log4Shell. Our cybersecurity team is actively investigating the impact of the vulnerability on Schneider Electric offers and will continuously update this notification as information becomes available.

In the meantime, customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from exploitation of this vulnerability. Where appropriate, this includes locating their systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks; and following the recommended mitigations and [general security recommendations](#) below.

Please subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification, including information on affected products and remediation plans:

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

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's [Customer Care Center](#).

October 2022 Update: A remediation is now available for Netbotz 750/755 ([page 4](#)).

Details

Log4j is an open-source Java logging library developed by the Apache Foundation which is widely used by both enterprise applications and cloud services. The recent Apache Log4j vulnerabilities are listed below and have ratings ranging from High to Critical. [CVE-2021-44228](#) (Log4Shell), received a rating of Critical and can allow an attacker who can control log messages or log message parameters to execute arbitrary code loaded from LDAP servers and other JNDI related endpoints when message lookup substitution is enabled. Exploitation could allow for unauthenticated remote code execution (RCE) and possibly access to servers. Additional CVEs within the scope of this security notification:

[CVE-2021-44228](#)

[CVE-2021-45046](#)

[CVE-2021-45105](#)

[CVE-2021-4104](#)

[CVE-2021-44832](#)

For more information, please visit the Apache logging services Log4j security page <https://logging.apache.org/log4j/2.x/security.html>.

Schneider Electric Security Notification

Affected Products, Remediations & Mitigations

As of the date of this publication, Schneider Electric has determined that the following offers are impacted and has provided remediations for those listed in the [Available Remediations](#) section, and recommended mitigations for those in the [Affected Products](#) section. Our cybersecurity team continues to actively investigate the impact on Schneider Electric offers and will update this notification as information becomes available.

For additional information and support, please contact your Schneider Electric sales or service representative or [Schneider Electric's Customer Care Center](#).

Available Remediations

Affected Products & Versions	CVEs	Remediations
APC PowerChute Business Edition PCBE <i>Software Versions: 9.5, 10.0, 10.0.1, 10.0.2, 10.0.3, and 10.0.4</i>	CVE-2021-44228 CVE-2021-45046	<p>PowerChute Business Edition V10.0.5 has been updated with Log4j V2.17.0 which includes a fix for these vulnerabilities and can be downloaded here: https://www.apc.com/shop/us/en/products/PowerChute-Business-Edition-v10-0-5/P-SFPCBE1005</p> <p>10.0.5 Release Notes: https://download.schneider-electric.com/files?p_File_Name=990-3029P-EN.pdf&p_Doc_Ref=SPD_CCON-AT6CWT_EN&p_enDocType=User+guide</p> <p>For more information, please see this FAQ: https://www.apc.com/my/en/faqs/FAQ000229596/</p>
APC PowerChute Network Shutdown (PCNS) <i>PCNS Software Versions: 4.4.1, 4.4, 4.3, and 4.2</i>	CVE-2021-44228 CVE-2021-45046	<p>For PowerChute Network Shutdown customers who would like to use Dell VxRail enabled NMC cards, please update to version PCNS 4.5 or later, which includes a fix for these vulnerabilities. Otherwise, customers on PowerChute Network Shutdown V4.3, 4.4, and V4.4.1 should follow these remediations steps:</p> <ul style="list-style-type: none"> Download the corresponding V4.4.1.1, V4.4.0.1, V4.3.0.1 scripts and follow the instructions available at https://www.apc.com/my/en/faqs/FAQ000229596/. These scripts remove the vulnerable Log4j files and replace them with Log4j V2.17.1 files, which include a fix for these vulnerabilities.

Schneider Electric Security Notification

EcoStruxure™ IT Gateway V1.5.0 - V1.13.1.5	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	V1.13.2.3 of EcoStruxure™ IT Gateway has been updated with Log4j 2.17.0, which includes a fix for these vulnerabilities, and is available via automatic update if enabled. Update manually by logging into EcoStruxureit.com, or by downloading the update directly from here: https://EcoStruxureit.com/download-and-set-up-EcoStruxurit-gateway/
EcoStruxure™ IT Expert Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	The cloud-based EcoStruxure™ IT Expert has been updated has been updated with Log4j V2.17, which includes a fix for these vulnerabilities. These fixes have been deployed automatically and require no action from customers.
EMA Server Cloud	CVE-2021-44228	Schneider Electric has deployed a fix to update EMA Server cloud offer to Log4j V2.17.1. These fixes have been deployed automatically and require no action from customers.
Eurotherm Data Reviewer V3.0.2 software or earlier	CVE-2021-44228	V4.0.0 of Eurotherm Data Reviewer includes a fix for this vulnerability and is available for download here: https://www.eurotherm.com/?wpdmdl=78469
Facility Expert Small Business Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update the Facility Expert Small Business cloud application to Log4j V2.17. These fixes have been deployed automatically and require no action from customers.
Harmony Configurator V33 and prior	CVE-2021-44228, CVE-2021-45046, CVE-2021-45105	Harmony Configurator has been updated with Log4j V2.17, which includes a fix for these vulnerabilities. These fixes have been deployed automatically and require no action from customers.

Schneider Electric Security Notification

MSE <i>Cloud</i>	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	<p>Schneider Electric has deployed a fix to update MSE to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>
NetBotz 750/755 <i>Software</i> V5.0.0 - V5.3.0	CVE-2021-44228 CVE-2021-45046	<p>For software V5.0.1 - 5.3.x of Netbotz 750/755 there is a patch that includes a fix for this vulnerability.</p> <p>The patch is available through your local tech support who can be reached here:</p> <p>https://www.se.com/ww/en/work/support/country-selector/contact-us.jsp</p>
SDK-Docgen <i>Cloud</i>	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	<p>Schneider Electric has deployed a fix to update SDK-Docgen to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>
SDK-UMS <i>Cloud</i>	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	<p>Schneider Electric has deployed a fix to update SDK-UMS to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>
Select and Config DATA <i>Cloud</i>	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	<p>Schneider Electric has deployed a fix to update Select and Config DATA to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>
SNC-API <i>Cloud</i>	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	<p>Schneider Electric has deployed a fix to update SNC-API to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>

Schneider Electric Security Notification

<p>SNC-CMM <i>Cloud</i></p>	<p>CVE-2021-44228 CVE-2021-45046 CVE-2021-45105</p>	<p>Schneider Electric has deployed a fix to update SNC-CMM to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>
<p>SNC-SEMTECH <i>Cloud</i></p>	<p>CVE-2021-44228 CVE-2021-45046 CVE-2021-45105</p>	<p>Schneider Electric has deployed a fix to update SNC-SEMTECH to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>
<p>TwinBus IP (formerly Digides 2.0) <i>Cloud</i></p>	<p>CVE-2021-44228 CVE-2021-45046 CVE-2021-45105</p>	<p>Schneider Electric has deployed a fix to update TwinBus IP to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>
<p>Workplace Advisor <i>All versions</i></p>	<p>CVE-2021-44228</p>	<p>Schneider Electric has deployed a fix to update Workplace Advisor to Log4j V2.17.</p> <p>These fixes were deployed implemented on all public facing portals on January 14, 2022, and require no action from customers.</p>
<p>Wiser™ by SE Platform <i>Cloud</i></p>	<p>CVE-2021-44228 CVE-2021-45046 CVE-2021-45105</p>	<p>Schneider Electric has deployed a fix to update the Wiser by SE Platform to Log4j V2.17.</p> <p>These fixes have been deployed automatically and require no action from customers.</p>

Customers should use appropriate patching methodologies when applying patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of 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.

Affected Products

Schneider Electric is currently establishing a remediation plan for the following products. This document will be updated when product specific information is available. Until then, customers should immediately apply the provided mitigations to reduce the risk of exploit. Our cybersecurity team continues to actively investigate the impact on Schneider Electric offers and will update this notification as information becomes available.

Schneider Electric Security Notification

For additional information and support, please contact your Schneider Electric sales or service representative or [Schneider Electric's Customer Care Center](#).

Affected Products & Version	CVEs	Recommended Mitigations
<p>Eurotherm Data Reviewer V3.0.2 and prior</p>	<p>CVE-2021-45046</p>	<p>Schneider Electric is establishing a remediation plan for all future versions of Eurotherm Data Reviewer 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 mitigations found in the document below to reduce the risk of exploit:</p> <p>https://download.schneider-electric.com/files?p_Doc_Ref=EDR-Log4Shell-Mitigations</p> <p>The above settings change will not alter the behavior of the Eurotherm Data Reviewer software</p> <p><i>Note: Eurotherm Data Reviewer uses a defense-in-depth strategy for security. It is currently not possible to exploit this vulnerability without logging into the server hosting Reviewer with administrator privileges.</i></p>

Recommended Mitigations

Customers should use an IoT/OT-aware network detection and response (NDR) solution and SIEM/SOAR solution to auto-discover and continuously monitor devices for anomalous or unauthorized behaviors, such as communication with unfamiliar local or remote hosts.

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.

Schneider Electric Security Notification

- 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.

Resources

<https://logging.apache.org/log4j/2.x/security.html>.

<https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance>

<https://cyber.gc.ca/en/alerts/apache-security-advisory-4>

<https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited/>

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, please contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

<https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.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 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 <i>13 December 2021</i>	Original Release
Version 2.0 <i>15 December 2021</i>	EcoStruxure™ IT Gateway and EcoStruxure™ IT Expert added to available remediations section.
Version 3.0 <i>16 December 2021</i>	APC PowerChute Business Edition and APC PowerChute Network Shutdown added to affected products section.
Version 4.0 <i>17 December 2021</i>	Overview updated to include CVE-2021-45046, Facility Expert Small Business and Wiser by SE platform added to list of available remediations, EASYFIT, Ecoreal XL, Eurotherm Data Reviewer, MSE, NetBotz750/75, NEW630, SDK BOM, SDK-Docgen, SDK-TNC, SDK-UMS, SDK3D-2DRenderer, SDK3D-360Widget, SNC-API, SNC-CMM, SNC-SEMTECH, SPIMV3, SWBEditor, SWBEngine added to list of affected products.
Version 5.0 <i>21 December 2021</i>	CVE-2021-4104 added to the scope of this security notification.
Version 6.0 <i>23 December 2021</i>	<ul style="list-style-type: none"> - Updated information for Facility Expert Small Business and Wiser by SE Platform in available remediations section. - Workplace Advisor added to list of affected offers.

Schneider Electric Security Notification

<p>Version 7.0 <i>23 December 2021</i></p>	<ul style="list-style-type: none"> - Updated information for Facility Expert Small Business and Wisier by SE Platform and added Harmony Configurator, MSE, NetBotz750/755, SDK-Docgen, SDK-UMS, SNC-API, SNC-CMM, SNC-SEMTECH to list available remediations. - Upon further investigation the following products have been determined to not be affected by the Log4j vulnerabilities and have been removed from the list of affected offers: EASYFIT, Ecoreal XL, NEW630, SDK BOM, SDK-TNC , SDK3D-2DRenderer, SDK3D-360Widget, SPIMV3, SWBEditor, SWBEngine.
<p>Version 8.0 <i>24 December 2021</i></p>	<p>Added TwinBus IP (formerly Digides 2.0) and Select and Config DATA to list available remediations.</p>
<p>Version 8.1 <i>29 December 2021</i></p>	<p>Added CVE-2021-44832 to the scope of this security notification.</p>
<p>Version 9.0 <i>13 January 2022</i></p>	<p>Remediations updated for EcoStruxure™ IT Gateway & EcoStruxure™ IT Expert to address CVE-2021-45105.</p>
<p>Version 10.0 <i>01 February 2022</i></p>	<p>Netbotz remediation updated due to stability issue on version 5.3.1.</p>
<p>Version 11.0 <i>08 March 2022</i></p>	<p>Remediation available for APC PowerChute Business Edition, APC PowerChute Network Edition, and EMA Server.</p>
<p>Version 12.0 <i>30 March 2022</i></p>	<p>Remediation update for Workplace Advisor.</p>
<p>Version 13.0 <i>09 August 2022</i></p>	<p>Remediation now available for Eurotherm Data Reviewer.</p>
<p>Version 14.0 <i>11 October 2022</i></p>	<p>A remediation is now available for Netbotz 750/755 (page 4).</p>