Schneider Electric Security Notification

Apache Log4j Vulnerabilities (Log4Shell)

13 December 2021 (13 January 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.

January 2022 Update: Remediations updated for *EcoStruxure IT Gateway and EcoStruxure IT Expert* to address CVE-2021-45105 (page 2).

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

Schneider Electric Security Notification

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

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 & Version	CVEs	Remediation/Mitigation
EcoStruxure IT Gateway V1.5.0 to V1.13.1.5	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Version 1.13.2.3 of EcoStruxure IT Gateway has been updated with log4j V2.17.0, which includes a fix for these vulnerabilities, and is available via automatic update if enabled, updating manually by logging into ecostruxureit.com, or by downloading the update directly from here: *https://ecostruxureit.com/download-and-set-up-ecostruxureit-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. No customer action is required.
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 2.17. These fixes have been deployed automatically and require no action from customers.

Schneider Electric Security Notification

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. No further action is needed from customers.
MSE Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update MSE to Log4j 2.17. These fixes deployed automatically and require no action from customers.
NetBotz750/755 Software versions 5.0 through 5.3.0	CVE-2021-44228 CVE-2021-45046	V5.3.1 has been updated with log4j V2.16, which includes a fix for these vulnerabilities, and is available for download here: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=NBRK075x_Build_5.3.1.175.sedp&p_Doc_Ref=APC_SFNBZ_531_EN
SDK-Docgen Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update SDK-Docgen to Log4j 2.17. These fixes deployed automatically and require no action from customers.
SDK-UMS Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update SDK-UMS to Log4j 2.17. These fixes deployed automatically and require no action from customers.
Select and Config DATA Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update Select and Config DATA to Log4j 2.17. These fixes deployed automatically and require no action from customers.
SNC-API Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update SNC-API to Log4j 2.17. These fixes deployed automatically and require no action from customers.

Schneider Electric Security Notification

SNC-CMM Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update SNC-CMM to Log4j 2.17. These fixes deployed automatically and require no action from customers.
SNC-SEMTECH Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update SNC-SEMTECH to Log4j 2.17. These fixes deployed automatically and require no action from customers.
TwinBus IP (formerly Digides 2.0) Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update TwinBus IP to Log4j 2.17. These fixes deployed automatically and require no action from customers.
Wiser by SE Platform Cloud	CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	Schneider Electric has deployed a fix to update the Wiser by SE Platform to Log4j 2.17. These fixes have been deployed automatically and require no action from customers.

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.

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 Mitigation
APC PowerChute Business Edition **PCBE Software Versions: 9.5, 10.0, 10.0.1, 10.0.2, 10.0.3, and 10.0.4**	CVE-2021-44228 CVE-2021-45046	Customers should immediately apply the following mitigations to reduce the risk of exploit: **Windows:** 1. Download and install 7-Zip from https://www.7-zip.org/download.html 2. Open a cmd prompt as Administrator. 3. Change directory to: `C:\Program Files (x86)\APC\PowerChute Business Edition\agent\lib` 4. Stop the PowerChute service: `net stop apcpbeagent` 5. Run the following command: `"c:\Program Files\7-Zip\7z.exe" d` **`log4j-core-2.14.1.jar`** `JndiLookup.class -r` 6. Start the PowerChute service `net start apcpbeagent` **NOTE**: For versions 10.0, 10.0.1, 10.0.2 replace the text in bold with `log4j-core-2.11.1.jar` and for version 9.5 replace this with `log4j-core-2.2.jar`. **Linux/PowerChute Virtual Appliance:** 1. SSH to the PowerChute machine as root user. 2. Change directory to `/opt/APC/PowerChuteBusinessEdition/Agent/lib folder` 3. Stop the PowerChute daemon using this command: `service pbeagent stop` or `/etc/init.d/PBEAgent stop` or `systemctl stop PBEAgent` (This will depend on the version of Linux) 4. Run the following command: `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class` 5. Re-start the PowerChute service: `service pbeagent start` or `/etc/init.d/PBEAgent start,` or `systemctl start PBEAgent` **NOTE:** If the "zip" command is not available you may need to install the application using a package manager such as yum, apt-get or zypper depending on the version of Linux you are running. To do this on RedHat Linux for example: 1. `yum install unzip` (this is a dependency of the zip tool) 2. `yum install zip`

APC PowerChute Network Shutdown (PCNS) **PCNS Software Versions - 4.4.1, 4.4, 4.3, and 4.2**	CVE-2021-44228 CVE-2021-45046	Customers should immediately apply the following mitigations to reduce the risk of exploit: **Windows:** 1. Download and install 7-Zip from https://www.7-zip.org/download.html 2. Open a command prompt as Administrator. 3. Change directory to: `C:\Program Files\APC\PowerChute\group1\lib` 4. Stop the PowerChute service: `net stop pcns1` 5. Run the following command: `"c:\Program Files\7-Zip\7z.exe" d` **`log4j-core-2.13.3.jar`** `JndiLookup.class -r` 6. Start the PowerChute service `net start pcns1` **NOTE**: For V4.3 replace the text in bold with `log4j-core-2.10.0.jar` and for V4.2 replace this with `log4j-core-2.2.jar`. **Linux/PowerChute Virtual Appliance:** 1. SSH to the PowerChute machine as root user. 2. Change directory to: `/opt/APC/PowerChute/group1/lib folder` 3. Stop the PowerChute daemon using this command – `service PowerChute stop` 4. Run the following command: `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class` 5. Re-start the PowerChute service: `service PowerChute start` **NOTE:** If the “zip” command is not available you may need to install the application using a package manager such as yum, apt-get or zypper depending on the version of Linux you are running. To do this on the PowerChute Virtual appliance for example: 1. `yum install unzip` (this is a dependency of the zip tool) 2. `yum install zip`

Schneider Electric Security Notification

Workplace Advisor **All versions**	CVE-2021-44228	Schneider Electric is currently working on a fix to update Building Advisor StarDog to Log4j 2.17. In the meantime, customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from exploitation of this vulnerability. For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.
Eurotherm Data Reviewer **V3.0.2 and prior**	CVE-2021-44228 CVE-2021-45046	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: https://download.schneider-electric.com/files?p_Doc_Ref=EDR-Log4Shell-Mitigations The above settings change will not alter the behavior of the Eurotherm Data Reviewer software *Note that 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.*

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.
- 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

Schneider Electric Security Notification

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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *13 December 2021*	Original Release
Version 2.0 *15 December 2021*	EcoStruxure IT Gateway and EcoStruxure IT Expert added to available remediations section
Version 3.0 *16 December 2021*	APC PowerChute Business Edition and APC PowerChute Network Shutdown added to affected products section
Version 4.0 *17 December 2021*	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 *21 December 2021*	CVE-2021-4104 added to the scope of this security notification.
Version 6.0 *23 December 2021*	- Updated information for Facility Expert Small Business and Wiser by SE Platform in available remediations section (page 3) - Building Advisor StarDog added to list of affected offers (page 6)

Schneider Electric Security Notification

Version 7.0 *23 December 2021*	- Updated information for *Facility Expert Small Business* and *Wiser by SE Platform* and added *Harmony Configurator, MSE, NetBotz750/755, SDK-Docgen, SDK-UMS, SNC-API, SNC-CMM, SNC-SEMTECH* to list available remediations. (page 3-4) - Added *Building Advisor StarDog* to the list affected offers. (page 7) - 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*
Version 8.0 *24 December 2021*	- Added *TwinBus IP (formerly Digides 2.0)* and *Select and Config DATA* to list available remediations. (page 3 and 4)
Version 8.1 *29 December 2021*	Added CVE-2021-44832 to the scope of this security notification (page 1)
Version 9.0 *13 January 2022*	Remediations updated for EcoStruxure IT Gateway & EcoStruxure IT Expert to address CVE-2021-45105.

Product Security Office

Digitally signed by Product Security Office
Date: 2022.01.12 17:52:51 -05'00'