Apache Log4j Vulnerability (Log4Shell)

13 December 2021

Overview

Schneider Electric is aware of the vulnerability known as Log4Shell impacting Apache Log4j, an open-source code project frequently used by applications and services from a variety of vendors. Our cybersecurity team is actively investigating its potential impact on Schneider Electric offers.

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 updates to this bulletin:


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

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 vulnerability impacting Apache Log4j is tracked as CVE-2021-44228 and received a rating of Critical. An attacker who can control log messages or log message parameters can 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.

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

Recommended Mitigations

Schneider Electric continues to assess how the Log4j vulnerabilities affect its offers, and will update customers through its Cybersecurity Support Portal as product-specific mitigation information becomes available.
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.

Resources

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

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, 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


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

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:

<table>
<thead>
<tr>
<th>Version 1</th>
<th>Original Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 December 2021</td>
<td></td>
</tr>
</tbody>
</table>

Product Security Office

Digitally signed by Product Security Office
Date: 2021.12.13 11:09:03 -05'00'