TECHNICAL BULLETIN TB-2021-12-23

Remediating Log4j Vulnerabilities in Components Distributed with Adept

12/23/2021

Synergis Software

A Division of Synergis Technologies, LLC

Suite 100, 18 South 5th Street

Quakertown, Pennsylvania 18951 U.S.A.

800.836.5440 / 215.302.3000

www.SynergisSoftware.com

WARNING AND DISCLAIMER

This document is designed to provide information about Adept Document Management. Every effort has been made to make it as complete and as accurate as possible. However, no warranty of suitability, purpose or fitness regarding this document or the software described is made or implied. The authors and Synergis Software shall have neither liability nor responsibility to any person or entity with respect to loss or damages in connection, with or arising from, the information contained in this document.

TECHNICAL BULLETIN VERSION HISTORY

	Release Date	Description
	12/23/2021	Review, edits incorporated
	12/20/2021	Initial release

SUMMARY

On 12/14/2021, we issued a Technical Bulletin entitled “CVE-2021-44228 Log4Shell - Log4j Remote Code Execution” that provided guidance on mitigating vulnerabilities in Log4J components distributed with Adept. Since then, critical information has come to light that supersedes the information provided in that communication.

We now know that additional remediation steps are required to eliminate all currently identified vectors for malicious code insertion in Log4J.

This communication represents the most current information as of 12/23/2021. This guidance, including the Log4J Mitigation Utility available from the Synergis Software Customer Portal, is designed to help you eliminate all currently known Log4J vulnerabilities.

AFFECTED PRODUCT VERSIONS

All versions of Adept using the Oracle AutoVue version 21 or higher are affected. The integrated Oracle AutoVue viewer uses an affected version of the Log4J component, as do the integration components. Since AutoVue is deployed on workstations and servers, **run the Utility on all workstations and servers on which Adept is installed.**

Affected product versions:

	Adept Product	Version	Release Date
	Adept 2015 SP3	10.0.3.11	1/18/2016
	Adept 2015 SP4	10.0.4.34	4/1/2016
	Adept 2017	10.1.0.151	9/6/2016
	Adept 2017 SP1	10.1.1.72	12/9/2016
	Adept 2017 SP2	10.1.2.127	4/19/2017
	Adept 2017 SP3	10.1.3.55	6/30/2017
	Adept 2018	11.0.0.405	7/31/2018
	Adept 2018.1	11.0.1.202	2/15/2019
	Adept 2018 UP1	11.0.0.420	10/25/2018
	Adept 2019	11.0.2.209	10/4/2019
	Adept 2019.1	11.0.3.179	4/2/2020
	Adept 11.0.4	11.0.4.528	10/18/2021

CVES REMEDIATED USING THE LOG4J MITIGATION UTILITY

The following reported issues are remediated by the Utility, using the mitigation approaches listed. Please note that the Utility addresses three Log4J CVE's and remediates affected components in Log4J 1.x and Log4J 2.x per the table below. You can find additional details regarding Apache's recommended mitigations here: Apache Log4j Security Vulnerabilities.

National Vulnerabilities Database CVE Number	Log4J 1.x Mitigation Implemented	Log4J 2.x Mitigation Implemented	Affected Components
CVE-2021-44228	**Remove** JMSAppender.class from Log4J distribution	**Remove** JndiLookup.class from Log4J distribution	AutoVue Desktop Deployment, AutoVue Web Client, Adept → AutoVue Integration, Tomcat on the webserver
CVE-2021-45046	Log4J1.x not affected	**Remove** JndiLookup.class from Log4J distribution	AutoVue Desktop Deployment, AutoVue Web, Tomcat on the webserver
CVE-2019-17571	**Remove** SocketServer.class, JMSAppender.class, SMTPAppender$1.class, and SMTPAppender.class from the Log4J distribution	Log4J2.x not affected	AutoVue Desktop Deployment, AutoVue Web Client, Adept → AutoVue Integration, Tomcat on the webserver

Please note that these mitigations can be performed manually. However, the Utility automates the removal of all affected Java classes on a machine deployed in multiple locations.

SERVERS AND WORKSTATIONS REQUIRING MITIGATION

To mitigate all current known vectors for exploiting vulnerabilities in Log4J components distributed with Adept as of 12/22/2021, run the Utility on all **servers** on which Adept is installed **and** on all **workstations** on which the Adept Desktop Client is installed.

This includes:

- The server on which the Native Adept Server is installed
    - The Adept Desktop client is commonly installed on the server running the Native Adept Server service, and therefore also may have the viewer installed.
- The web server on which the Adept Web Application and Adept Web Server are installed

Workstations that use a web browser to access Adept (Explorer, Reviewer, and Creator licenses) must also be remediated separately for Java vulnerabilities. The Viewer included with Adept Web uses a Java deployment from Java.com. Fixes provided by Oracle from Java.com must be deployed to mitigate

vulnerabilities on these workstations, as these Java installations are a prerequisite for viewing in the web client and not distributed by Synergis Software.

COMPONENTS NOT REMEDIATED USING THE UTILITY

Components **not** remediated by the Utility:

- Installed components copied and pasted to different folders other than the root of Adept Installation folders. *
    - Java versions downloaded from Java.com installed on workstations or servers as machine wide JREs. These Java deployments must be mitigated using fixes provided by Oracle.
- Installed components copied and renamed to different names, i.e. “log4j.jar” renamed to “log4j.old”
- Instances of Log4J installed by non-Adept installers and applications. *
- Installed versions of Adept backed up using any backup solution
- The Utility **does not** alter any Adept Installation MSIs.
    - If a new installation of Adept is performed, it must be immediately remediated using the Utility.
    - Synergis Software will provide customers with updated Fall 2021 Adept (11.0.4) installation packages via the Synergis Software Customer Portal once validated; however, there are no current plans to update earlier Adept version installations.

* *Although the Utility provides a “Forced Directory Mode” flag, which can be set when running the application in Silent Mode, Synergis does not support modifying other vendors’ distributed Log4J components. Use this at your own risk!*

NEXT STEPS

Please download the Utility from the Synergis Software Customer Portal to help you eliminate all currently known Log4J vulnerabilities. Instructions are included in the download package. If you have any questions, please do not hesitate to contact Helpdesk.

DATA PROTECTION FOCUSED

Data protection is a top priority at Synergis Software. Security vulnerabilities, such as the Log4J vulnerability and those experienced by SolarWinds and Kaseya more recently, are on the rise. In the ordinary course of business, our teams continuously revisit our procedures and protocols, and we reevaluate them when new vendor vulnerabilities, such as these, are exposed. We employ routine and targeted penetration testing, have implemented strong encryption through our SSL Everywhere option for data in transit, provide advanced TLS support, offer CORS protection, are compatible with best-in-class encryption at rest solutions, and practice many other hardening techniques to keep your data safe.

Thank you for being a valued customer.