Vulnerability in Apache Log4j Library Affecting Bizerba Products: December 2021

BIZERBA-SA-2021-0003
Monday 13th December 2021

Update 2 of this document is highlighted in yellow (Monday 13th December 2021).
Update 3 of this document is highlighted in green (Tuesday 14th December 2021).
Update 4 of this document is highlighted in turquoise (Thursday 16th December 2021).
Update 5 of this document is highlighted in magenta (Tuesday 21th December 2021).
Update 6 of this document is highlighted in red (Thursday 13th January 2022).
Update 7 of this document is highlighted in grey (Tuesday 18th January 2022).

Overview

On December 9, 2021, the following vulnerability in the Apache Log4j Java logging library affecting all Log4j2 versions prior to 2.15.0 was disclosed:

> CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints

For a description of this vulnerability, see the Fixed in Log4j 2.15.0 section of the Apache Log4j Security Vulnerabilities page.

CVSS Rating
The CVSS v3.0 Base Score is rated at: 10 (Critical
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

1 Affected Products

Bizerba is investigating its product line to determine which products may be affected by this vulnerability. Depending on the progress of the investigation, Bizerba will update this notice with information about affected products.

This is an ongoing investigation, so please be aware that products that are currently considered non-vulnerable may later be determined to be vulnerable as additional information becomes available.

Retail

- Retail scales K3 (see below “Retail software” for affected versions)
- Retail scales K-Class (see below “Retail software” for affected versions)
- Retail scales X-Class (see below “Retail software” for affected versions)
- Retail scales M-Class (see below “Retail software” for affected versions)
- SmartShelf

Retail Packaging systems

- Wrapper B3

Retail software

- RetailApps
  - PaymentManager all versions below v1.58b0007 are affected
  - VoucherSystemCentral all versions below v1.54b0006 are affected
  - PowerQueuePosiflex all versions below v1.55b0002 are affected
  - PowerQueueLCD all versions below v1.55b0002 are affected
- PowerSuite >= 3.50 (log4j version 2.11.2)
- RetailStore >= 1.0 (log4j version 2.11.2)

Other products / other software

To our knowledge, no other of our products/software are affected by the vulnerability. Please contact us if you have any worries about a particular product. We are continuing to investigate the incident and will update this document.

Log4j 1.x

We have audited all products containing the Log4j library. For any known occurrence of the Log4j 1.x version, we mitigated the risk by auditing the source code as recommended by the Apache Log4j security team[3]. Up to now we have no indication that JMSAppender are used in any product. Therefore, our products containing Log4j 1.x are not impacted by this vulnerability[3].

Log4j 2.x hotfix mitigation:

Our current hotfix mitigates the vulnerability by setting the environment variable LOG4J_FORMAT_MSG_NO_LOOKUPS to true. Our internal tests confirmed the effectiveness of this measure. We reviewed the source code of the affected product and could not find any other attack paths mentioned[3] (e.g. Logger.printf("%s", userInput) or applications that use a custom message factory).

[3] https://logging.apache.org/log4j/2.x/security.html

Log4j 2.17 (CVE-2021-44832):

JDBC Appender is not used in our products. Therefore, our products are not affected by this vulnerability. Of course, we will include the latest version of the log4j library in the next scheduled release.

2 Vulnerability Fix

A hotfix patch is available for PowerSuite, RetailStore for all retail scales and B3 Wrapper for Windows OS[1] and Linux OS[2], and for the named RetailApps and SmartShelf. Please contact your local Bizerba partner/service organisation for a timely update.

[1] bizhotfixlog4j_v100_b0003_win_99999999100.zip
[2] bizretail_hotfixlog4j_v101_b0004_lin_99999999999.zip

In addition to the hotfix[1,2] a patch[4] is available to update log4j library to the latest version 2.17 for PowerSuite (>=3.50) and RetailStore (>=1.0) for Linux OS and Windows. The RetailApps PaymentManager, VoucherSystemCentral, PowerQueuePosiflex and PowerQueueLCD where also updated to the latest log4j version 2.17. Please contact your local Bizerba partner/service organisation for a timely update.

[4] bizretail_libpatcher_v001_b0012_00000000000.zip

A new version[5] of the patch[4] is available for PowerSuite (>=3.50) and RetailStore (>=1.0) for Linux OS and Windows. This patch updates the log4j library to the latest version 2.17.1. Please contact your local Bizerba partner/service organisation for a timely update.

[5] bizretail_log4jlibpatch_v001_b0018_00000000000.zip

3 Workarounds and Mitigations

Until the fix is completed, the risk can be mitigated by separating the devices or block access to vulnerable web services at network ports 8310, 8500, 8508 and 8509.

4 Further measures

We are updating products containing Log4j 1.x and Log4j 2.0–2.15 to the latest version ~~2.16~~ during scheduled next releases as regular update.

5 Links

[LUN2021] - RCE 0-day exploit found in log4j, a popular Java logging package
https://www.lunasec.io/docs/blog/log4j-zero-day/

[GIT2021b] - Vulnerability check script
https://gist.github.com/byt3bl33d3r/46661bc206d323e6770907d259e009b6

[GIT2021c] - Github release von Log4j
https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2