Apache Log4j Vulnerability – CVE-2021-44228: Customer key update document

Updated: Dec. 16, 2021 5:00 pm ET

Diebold Nixdorf is aware of the Apache Log4J vulnerability and is working to quickly assess any potential impact to the company and our clients. We are committed to keeping our customers safe and are working proactively to ensure our resiliency. We will share more detailed information with you related to your operating environment and any potential impacts as soon as we have completed our assessment

What is Apache Log4j/ Log4j2?

Apache Log4j is an open-source Java-based logging utility which is part of the Apache Logging Services, a project of the Apache Software Foundation. Log4j is one of several Java logging frameworks.

- **Impacted software:** Several Diebold Nixdorf software products also use this enterprise java logging framework (view more details on page 2-3).

Tables starting on page 2 contain product-specific details. Some key points:

1. Operations portfolio solutions (e.g., Vynamic View, Security and Cash Management) are not impacted.
2. VCP-Lite and VCP-Pro (as ProFlex4) are impacted with hotfixes provided on Dec. 14.
3. Transaction middleware hotfix available since Dec. 15, 2021
4. VCP-Pro (as VISTA) and VCP-Pro (as VCP6) are impacted with a hotfix provided on Dec. 16, and prepackaged variations with a hotfix available by Dec. 17.

The Ubiquity of Log4j within Java applications could create exposure of your DN software environment, depending on the product/version you have deployed. A detailed list of impact on Vynamic software is on page 2-3. Our security teams are aware of the vulnerability and are working with the product development teams to mitigate the risk from this Log4j vulnerability.

Notes: The suspicious file to look for is **log4j-core**-<version>.jar. File names like **log4j-api**-<version>.jar, **slf4j-over-log4j**-<version>.jar or similar **do not indicate** that log4j is even used within a product.

JNDI processing and lookup must be enabled for the system to be vulnerable. Disabling JNDI processing or removing JndiLookup Class from Log4J Library is an effective interim solution to mitigate the risk from this Log4j vulnerability.

An outbound access from the vulnerable server to the Internet is required for the vulnerability to be exploited by an external actor (this potentially reduces likelihood of exploit for certain products). As an immediate and interim compensating control, effective attack surface management can also be used to prevent exploitation.

Managed Services-related issues/mitigation:

As Managed Service (MS) products are identified as needing any actions relative to log4j, those products where Managed Services is responsible for providing updates to the customer will be communicated, scheduled and deployed.

For any required actions related to servers that support managed services products, Diebold Nixdorf will follow standard Change Control processes to implement hotfixes or mitigation steps to address the vulnerability.

If you are a MS customer and see that there are non-MS products that are also affected that reside in your unit's software stack, please follow Diebold Nixdorf-recommended guidance for each product listed in the tables below. If you are a MS Software Deployment Services customer, you can make a request via the standard process to have managed services assist in implementing the fix.

To mitigate vulnerabilities such as this affecting your institution in the future, DN Managed Services highly recommends implementation of our Hard Disk Encryption and Enhanced Intrusion Protection offerings to help protect against this and similar attack vectors.

Banking product-specific details/updates

Updated 12/16/21 – 1:00 p.m. ET

Vynamic Software	Impacted by Log4j Vulnerability	Versions Impacted	Information for Customers
• VCP-Lite	Yes	ProCash v3.1/30	Hot Info 4945 (replaces Hot Info 4944) containing Log4j 2.16.0 on Dec 14. Previous versions are not affected
• VCP-Pro (as ProFlex4)	Yes	4.2/20 and newer	Hotfix 4945 released Dec. 14. Older versions not impacted.

• VCP-Pro (as Vista)	Yes	5.3 and newer Inclusive of prepackaged (Network Solution) Note: Versions prior to 5.3 are not impacted by this vulnerability.	Only customers enabled for one of these products or services are impacted: • ProChip EMV • TM • Personalization • Transaction Automation Hotfix provided on Dec. 16 and will be available to all prepackaged customers on Dec. 17. Patch will be included in the next consolidated bugfix for each affected version as well.
• VCP-Pro (as VCP6)	Yes	6.0.0 to 6.0.8	Hotfix provided on Dec. 16. Patch will be included in the next consolidated bugfix for 6.0 as well.
• Agilis 3	Yes	EmPower 3.7 91x SP5 NDx SP7 HF21013 (applied to EmPower Base 3.7 / Agilis 91x SP5 / Agilis NDx SP 7)	Impacted only if using HF21013 All others: Update to HF19024 to close the immediate threat New hotfix will be coming, which will ship log4j 2.15.0 on Dec.17, 2021 for affected customers using HF21013.
• Transaction Switching	Yes	TM V2.x - V3.x	TM fixes for 2.2, 2.3 and 3.0 are available since December 15
• Terminal Driving	Yes	TM V2.x - V3.x	TM fixes for 2.2, 2.3 and 3.0 are available since December 15
• Transaction Middleware	Yes	TM2.x - 3.x	TM fixes for 2.2, 2.3 and 3.0 are available since December 15

• Teller Platform	Yes (for TM based architecture)	FONet, FOTop (old architecture) TM V2.x – V3.x (new architecture)	FONet, FOTop are not impacted. TM fixes for 2.2, 2.3 and 3.0 are available since December 15
• Campaign Management	Yes	Vynamic Marketing V2.0 – V2.2	PreLoader and Customer Importer Tool will include the 2.16 log4j update with same timing as VM server. Plan to update the following VM Versions with log4j 2.16.0 by Dec. 22, 2021 at the latest, but likely by Dec 17 barring any unexpected complications: - 2.1.9 - 2.1.14 - 2.1.12 - 2.1.4 - 2.1.5 For all other Versions, we can do this at customer or product manager's request.
• Personalization	Yes	TM V2.x - V3.x	TM fixes for 2.2, 2.3 and 3.0 are available since December 15
• Transaction Automation	Yes	TM V2.x - V3.x	TM fixes for 2.2, 2.3 and 3.0 are available since December 15
• ProAKT	No	-	Software is not impacted by this vulnerability.
• XPression IVT	No	-	Software is not impacted by this vulnerability.
• Commander	No	-	Software is not impacted by this vulnerability.
• Vynamic View	No	-	Software is not impacted by this vulnerability.

• Access Protection	No	-	Software is not impacted by this vulnerability.
• Intrusion Protection	No	-	Software is not impacted by this vulnerability.
• Hard Disk Encryption	No	-	Software is not impacted by this vulnerability.
• Cash Forecasting	No	CCO (Cash Cycle Optimizer)	Software is not impacted by this vulnerability.
• Cash Logistics	No	CCO (Cash Cycle Optimizer)	Software is not impacted by this vulnerability.

Managed Software	Impacted by Log4j Vulnerability	Versions Impacted	Information for Customers
• CSP	No	All	No known vulnerabilities have been recognized and no risk is present
• eService	No	All	No known vulnerabilities have been recognized and no risk is present
• Opteview	No	Axeda Platform 6.9.2 and earlier do not have the vulnerability (using log4j version 1.2.15 with existing configuration).	DN is utilizing Axeda Platform 6.9.0. No known vulnerabilities have been recognized and no risk is present
• Radia	Yes	All	No client-side vulnerabilities. Implementation of mitigation has occurred as of 12/15. Hotfix implementation planned per standard change control processes.
• SEP	Yes	SEPM 14.3	RFC in process to implement mitigation recommended by Broadcom

Retail Software - Product specific details

Updated 12/15/21 – 1:30 ET

Software	Impacted by Log4j Vulnerability	Versions Impacted	Information for Customers
Vynamic Checkout (former TP.net)	No	3.5 - 7.5	Software is not impacted by this vulnerability
Vynamic Engage	No	1.0 - 1.2	
Vynamic Compact (former Namos)	No	7.18 - 7.19	
TP Linux	No	2.2 – 2.8	
Vynamic Self-Service	No	8 – 14.3	
Vynamic Cash	No	1.3/30, 1.3/40, 1.3/41, 1.4/00, 1.5.x, 2.0.x, 2.1.x, 2.2.x, 2.3.x and 2.4.x.	