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

Updated: Jan. 27, 2022 4:30 pm ET

Diebold Nixdorf is quickly addressing the Apache Log4J vulnerability and 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 continue to share more detailed information with you related to your operating environment and any potential impacts as we develop fixes and assess any additional threats related to the Log4J vulnerability

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 3 contain product-specific details. Some key points:

1. Operations portfolio solutions (e.g., Vynamic View, Security and Cash Management) are not impacted.
2. Software solutions offered as a service (SaaS) and hosted in the cloud by Diebold Nixdorf (e.g., AllConnect Data Engine, IVTaaS) are not vulnerable to this threat as the files are not directly accessible. The company is also adding an additional layer of protection by adding unique firewall rules to target any attempts to gain access. As new software comes available, we will deploy as part of our normal deployment/update process.
3. VCP-Lite and VCP-Pro (as ProFlex4) are impacted with hotfixes provided on Dec. 14.
4. Transaction middleware hotfix available since Dec. 15, 2021
5. VCP-Pro (VISTA) and VCP-Pro (VCP6) are impacted with a hotfix provided on Dec. 16, and prepackaged variations with a hotfix available since 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 begins on page 3. Our security teams are addressing the Log4j vulnerability and are working with the product development teams to mitigate the risk.

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/hotfixes/updates

Updated 1/27/22 – 4:30 p.m. ET

***Hotfixes are available for impacted products and versions. Customers with maintenance and support contracts can get the security hotfixes via normal channels for software hotfixes. We strongly recommend customers to contact Diebold Nixdorf Software Maintenance & Support to assist with identifying applicability and integration. For immediate access, the hotfixes are additionally available at the following links:*

VCP-Lite (ProCash)
https://eportal.wincor-nixdorf.com/anonhttp/download/9FBjwuDrpaSjkV70IbrvYvizzycPtda1n8Ip3Kge9iPnrrKWm5s31XPC4Gdj43G5
VCP-Pro (ProFlex4)
https://eportal.wincor-nixdorf.com/anonhttp/download/9FBjwuDrpaSjkV70IbrvYvizzycPtda1n8Ip3Kge9iPnrrKWm5s31XPC4Gdj43G5
VCP-Pro (Vista):
https://eportal.wincor-nixdorf.com/anonhttp/download/LoHTlM8GwEBn9sqNdLI2ygx7ItyUNy2xOmmUyWYK01F6LXG31iqsyuTlOn9bJ1wO
VCP-Pro (VCP6):
https://eportal.wincor-nixdorf.com/anonhttp/download/LoHTlM8GwEBn9sqNdLI2ygx7ItyUNy2xOmmUyWYK01F6LXG31iqsyuTlOn9bJ1wO
Agilis 3 HF21064:
https://eportal.wincor-nixdorf.com/anonhttp/download/7o2jMNv77cXKTFUFoJfD5E4mOQzq0FEjuZrFhy1KNSWw98QVGn7ujt4LgEHSbV9N
Agilis 3 HF21067:
https://eportal.wincor-nixdorf.com/anonhttp/download/LGQ2Iai1WNEXygSgek6DyDxob9BnlEdW072qPD0OHCsHOe2LiBrWoNSggTgtidwt
Transaction Middleware:
https://eportal.wincor-nixdorf.com/anonhttp/download/Iv59Nt5rerKRYbk5dLPQyFDGL1on1ISx0tOEncD4TXqQhzAxPW9dR9gUOtll1KSh
Campaign Management (Vynamic Marketing)
https://eportal.wincor-nixdorf.com/anonhttp/download/DZMpbvw8UNL9zWMWFynLqKuKh3PtPBjlJcgzFp7iwbUt53XDWPRAwB220KoDThKt

Vynamic Software	Impacted by Log4j Vulnerability	Versions Impacted	Information for Customers
• VCP-Lite	Yes	ProCash v3.1/30	Hotfix 4945** (replaces Hot Info 4944) containing Log4j 2.16.0 on Dec 14. Previous versions are not affected
• VCP-Pro (ProFlex4)	Yes	4.2/20 and newer	Hotfix 4945** released Dec. 14. Older versions not impacted.
• VCP-Pro (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 is available to all prepackaged customers from Dec. 17. Patch will be included in the next consolidated bugfix for each affected version as well.
• VCP-Pro (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 EMV 7.0	Impacted only if using HF21013 or EMV 7.0 HF21064 provided on Dec. 17 for customers who applied HF21013.

		HF21013 (applied to EmPower Base 3.7 / Agilis 91x SP5 / Agilis NDx SP 7)	HF21067 provided on Dec. 17 for EMV 7.0
• 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	Fixes for the following VM versions, utilizing log4j 2.16.0, are available since Dec 17: - 2.1.4 - 2.1.5 - 2.1.9 - 2.1.12 - 2.1.14 For all other Versions, we can do this at customer's or product manager's request. Note: Fixes for PreLoader and Customer Importer Tool are included as part of the VM package delivery.
• 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 Services Banking -- Americas	Impacted by Log4j Vulnerability	Versions Impacted	Information for Customers
• CSP	No	All	No known vulnerabilities have been recognized and no risk is present
• eService	Yes	All	Client-side vulnerability for eServices. Agent side Inventory scan component requires an update to Log4j 2.16 in order to patch the latest DOS vulnerability – patch provided 12/16 and in testing
• 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

• Opteview Policy Manager	Yes	**Axeda Policy Server Versions that use the vulnerable log4j library versions, are: 6.9.3, 6.9.3.1, 6.9.3.2, 6.9.3.3, 6.9.3.4, 7.0.0.0**	Required on Customer side: Remove existing log4j libraries and add latest non-vulnerable log4j libraries 1. Stop Policy Server Application/Service 2. Stop the Policy Server Database Application/Service 3. Delete existing [log4j-api-*.jar and log4j-core-*.jar] library and add [log4j-api-2.17.0.jar and log4j-core-2.17.0.jar] in below locations: a) Ensure that permissions match with the original files after replacing the .jars Versions: 6.9.3, 6.9.3.1, 6.9.3.2, 6.9.3.3, 6.9.3.4, 7.0.0.0 <Installed_Location>\Tomcat\aps\common\lib <Installed_Location>\Tomcat\aps\webapps\flexui\WEB-INF\lib <Installed_Location>\Tomcat\hsqldb\webapps\hsqldb\WEB-INF\lib <Installed_Location>\Tomcat\aps\webapps\webservices\WEB-INF\lib Version: 7.1.0 <Installed_Location>\Tomcat\aps\common\lib <Installed_Location>\Tomcat\aps\webapps\apsui\WEB-INF\lib <Installed_Location>\Tomcat\hsqldb\webapps\hsqldb\WEB-INF\lib 4. Start the Policy Server Database Application/Service 5. Start Policy Server Application/Service https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-api/2.17.0/log4j-api-2.17.0.jar https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.17.0/log4j-core-2.17.0.jar
• Radia	Yes	All	No client-side vulnerabilities. Implementation of mitigation has occurred as of 12/15 on backend.
• SEP	Yes	SEPM 14.3	No client-side vulnerabilities. Implement mitigation on backend Sunday 12/19
• DN software to be deployed for MS Customers		VCP vista 5.4+ VCP vista 5.5+ eServices all	MS planning mass deploy starting Jan. 5, 2022 for all received / tested patches. Customers can request custom deploy prior to this.

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.	