Cascade Data Systems.

Subject: ALIAS Workstations and the Log4j Exploit Vulnerability.

Date: 18 January 2022.

Overview

Recently there have been reports of a security exploit in the use of the Log4j logging library. While there is a lot of information on the Internet about this Log4j vulnerability, along with examples of its use, the following is a brief overview as we understand it. The feature that opens this security vulnerability in the Log4j system was introduced around 2013 in version 2, and it potentially affects any software that uses Java and incorporates the logging library. This vulnerability could permit a remote attacker to log connection information if that remote attacker can access software on a server that is both (a) listening to a remote connection and (b) using an affected version of the Log4j library. Note that this means several things:

- Software that is not listening to connections from remote computers is not affected.
- Software that is not based on Java code, or that does not use the Log4j library is not affected.
- Software from prior to 2013 is not affected, even if it has Java components and uses the Log4j library.

While the vulnerability could theoretically also affect a computer that an attacker was able to gain physical access to, it still would not be exploitable if either of the last two items above were true.

The rest of this document details an assessment that Cascade Data Systems has performed as to the impact on this vulnerability on the security of ALIAS Workstations. Please note, though, that Cascade Data Systems is not an internet security firm: we are not experts in security or in the use of Log4j--our focus is on the measurement of petroleum catalysts. As such, we cannot give definitive statements about internet security or about the Log4j vulnerability: we can merely provide our assessment of the situation to the best of our understanding. Also note that what follows applies to ALIAS Workstations as they were originally configured by Cascade Data Systems, prior to shipment. Software or drivers that were installed or customized after that point may have introduced Log4j vulnerabilities that Cascade Data Systems can have no knowledge of.

ALIAS Sub-elements

The ALIAS software installed on ALIAS Workstations includes the following elements, and the vulnerability of each of these is discussed further below.

1. The ALIAS.EXE program, written in Borland/Embarcadero Delphi.
2. The CATSCAN.DLL dynamic link library, written in Microsoft Visual C.
3. The ALIAS.CHM Help File, a compiled Microsoft HTML Help file.
4. The ALIAS.INI file, a text file used for storing user settings.
5. The TWAIN optical scanner interface, a set of standards for communicating with and operating optical scanners that is maintained by the TWAIN Working Group.
6. Software Drivers provided by Epson for its optical scanners.
7. Hardware key encryption of the ALIAS executable and dynamic link library, provided by Thales/Gemalto/SafeNet/Aladdin Systems.
8. Microsoft Office, specifically the Excel application.
9. The Microsoft Windows Operating System.
10. A DELL computer that includes drivers and programs which DELL pre-installed.

Vulnerability Discussion

(1), (2): The code written by Cascade Data Systems (ALIAS.EXE and CATSCAN.DLL) does not directly log any data with Log4j. Our code does not in any direct way make use of Java (nor indirectly as far as we're aware). ALIAS.EXE is compiled under Embarcadero's Delphi (owned by Borland, prior to 2008), and CATSCAN.DLL is compiled under Microsoft's Visual C. Here are comments posted to the Embarcadero Delphi website written by Marco Cantu, a well-known Delphi expert:

> *Now, what does [the Log4j issue] mean for Embarcadero in general and RAD Studio in particular? Directly, not much. Software built in Delphi or C++Builder doesn't use or rely in any way on Java (with the exception of Android applications) and therefore doesn't use Log4j. More in general, Delphi and C++Builder create natively compiled applications, which are less subject to execution environment problems (here I'm referring to Java, .NET or JavaScript execution environments). However in this case the issue was not in the execution environment, but in a popular library, and RAD Studio developers use add-on components and third party libraries, like any other developer community does.*

CDS Note: To our knowledge, none of the libraries and add-on components we use make use of Java or the Log4j logger.

(3): Regarding the vulnerability of compiled help files that were compiled on the Microsoft HTML Help Workshop, this question is best directed to Microsoft. (Note: The HTML Help Workshop compiler which Cascade Data Systems uses was last updated in the early 2000's, well before the Log4j features that exposed a vulnerability were introduced, and therefore should pose no direct exposure to the Log4j vulnerability.) The most recent version of our compiled ALIAS Help File is available on our secure website https://www.ALIAScds.com. We have now removed from that help file any direct links to internet websites, to provide additional protection. (Only two websites were previously linked: the Occupational Safety & Health Administration website of the U.S. Department of Labor, and the ALIAS website mentioned just above. These direct links have now been removed.)

(4): ALIAS does not directly use any logging software commands, other than storing and retrieving settings and other values in the ALIAS.INI text file. ALIAS code does not even directly write anything to the Windows System Registry.

(5): Regarding the vulnerability of the TWAIN drivers, this question was directed to the TWAIN Working Group: https://twain.org/forums/topic/log4j-vulnerability/. Here is the received response:

> *Q: Does anyone know if TWAIN is vulnerable to the recently discovered Log4j exploit?*
> *A: None of the classic TWAIN open source code delivered by the TWAIN Working Group uses Log4j: Data Source Manager or Sample code. Scanner vendors and application developers are free to use whatever tools they want.*

CDS Note: Epson has built support for the TWAIN interface into its drivers, and according to Epson's assessment of their "firmware, drivers, and utilities" for scanners (see the entry for point 6 just below), there is no vulnerability to the Log4j exploit.

(6): Regarding the vulnerability of the Epson drivers, this question is best directed to Epson. From their website: https://www.epson.ee/viewcon/corporatesite/kb/index/KA-01752

> *On December 22, 2021, we completed the impact investigation of this vulnerability for all Epson products (hardware, software) and all services including the cloud. As a result of the investigation, it was confirmed that all Epson products and services are not affected by this vulnerability.*
> *Epson product category for which the survey has been completed. Includes all software such as firmware, drivers, and utilities installed in respect of the hardware of the following products.*
> *[A long list of items that were investigated are given, and this list includes "Scanner".]*

(7) Thales responded as follows when specifically asked about this question with our new hardware encryption in use on ALIAS version 3.8.5.0:

> ***Q:*** *We've used only the LDK Envelope 8.2 on our code with the default settings (IIRC). We don't use EMS or anything else. Does this new vulnerability affect us? (I don't understand what your issue description is saying, so I can't tell.) And if it does affect us, how are we supposed to claw back all copies of our executables from our customers? Thank you. [I'm referring to the tech support email you sent out today: CVE-2021-44228 - Security vulnerability in Log4j affecting Sentinel LDK-EMS 8.x and how to mitigate it.]*
> ***A:*** *The affected component is LDK-EMS and Client-side applications are not affected by this vulnerability. Later today we will release a patch for LDK 8.3 (on Windows) for on-premises customers via Sentinel Up and will also patch LDKaaS for hosted customers. Customers who use LDK 8.0 and 8.2 will need to upgrade to LDK 8.3 to be able to install the patch.*
> ***Q:*** *Thank you. So are you saying that our enveloped code is protected just fine and that we don't need to make any changes?*
> ***A:*** *Yes your understanding is Correct.*
> 2021-12-13 13:49:33

Regarding the earlier Gemalto Hardware Keys, Thales responded as follows. *Note: Thales purchased Gemalto in 2019: https://www.thalesgroup.com/en/group/journalist/press-release/thales-completes-acquisition-gemalto-become-global-leader-digital. And depending on the age of a given ALIAS system, Gemalto was previously owned by SafeNet (which Gemalto purchased in 2014), and before that by Aladdin Systems (which SafeNet purchased in 2009). We asked Thales about these older hardware keys and this is their response:*

> ***Q:*** *We have products in the field that use Gemalto Sentinel Basic DL keys. The only use we make of them is to envelope our executables and DLLs. Would this create any Log4j exploit vulnerabilities for us? (Gemalto, of course, was recently purchased by Thales: that's why we're directing this question to you, as there is no one else to ask.) We also have older keys that were acquired from SafeNet before Gemalto purchased them: would you expect the answer to be any different for those keys? (From SafeNet, prior to 2016, we purchased HASP HL Basic keys.)*
>
> ***A:*** *As long as you use the latest Runtime/Driver for your keys there should be no vulnerabilities. Does not matter where you bought the keys nor how old they are. The current version is 8.31. The runtime driver is backward compatible so there should not be any problems if you need to install it. There were vulnerabilities in past versions of the Runtime. You can refer to the following document to view any vulnerabilities that existed in older versions:*
>
> *https://docs.sentinel.thalesgroup.com/ldk/LDKdocs/RTE_History/Content/New-Win.htm*
>
> *The Windows download for the GUI runtime installer is here:*
>
> *https://supportportal.thalesgroup.com/csm?sys_kb_id=61fb0ee1dbd2e78cfe0aff3dbf9619ab&id=kb_article_view&sysparm_rank=2&sysparm_tsqueryId=8713962ddbc501105d310573f396192c&sysparm_article=KB0018320*
>
> *If you open the PDF you can search for vulnerabilities and you will see what versions had vulnerability issues. It's always recommended to use the latest version as bug/vulnerability fixes are continually being made.*

CDS Note: We searched the list of vulnerabilities for "Log4j" and got no hits. (Our understanding is that data logging is something that's done with more advanced hardware keys and with software like Thales' Entitlement Management System (EMS), which ALIAS does not use.)

(8), (9): Regarding the vulnerability of Microsoft Office and of Microsoft Windows, this question is best directed to Microsoft. This is a good place to start: https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

(10): Regarding the vulnerability of any software or drivers that may have been initially installed on the computer by DELL, this question is best directed to DELL. The following website would be a good place to start: https://www.dell.com/support/kbdoc/en-us/000194414/dell-response-to-apache-log4j-remote-code-execution-vulnerability.

Summary
ALIAS is designed to be used on a standalone computer, and the code we've written does not directly access the internet in anyway (except for in the ALIAS Help File as mentioned above). We cannot address the vulnerability of any other software you may have installed on your ALIAS Workstations.

Cascade Data Systems recommends that you apply whatever patches and updates are recommended by Microsoft, Epson, Thales, and DELL to address the Log4j vulnerability issue. We believe ALIAS should continue to work properly if you do so. (To date, there have been no reports that patches or updates from these companies have had any adverse effect on the operation of ALIAS.)

Furthermore, if you have access to a reputable and trustworthy software tool that scans for Log4j vulnerabilities, then using it on your ALIAS units certainly seems like a prudent precaution.

--Cascade Data Systems