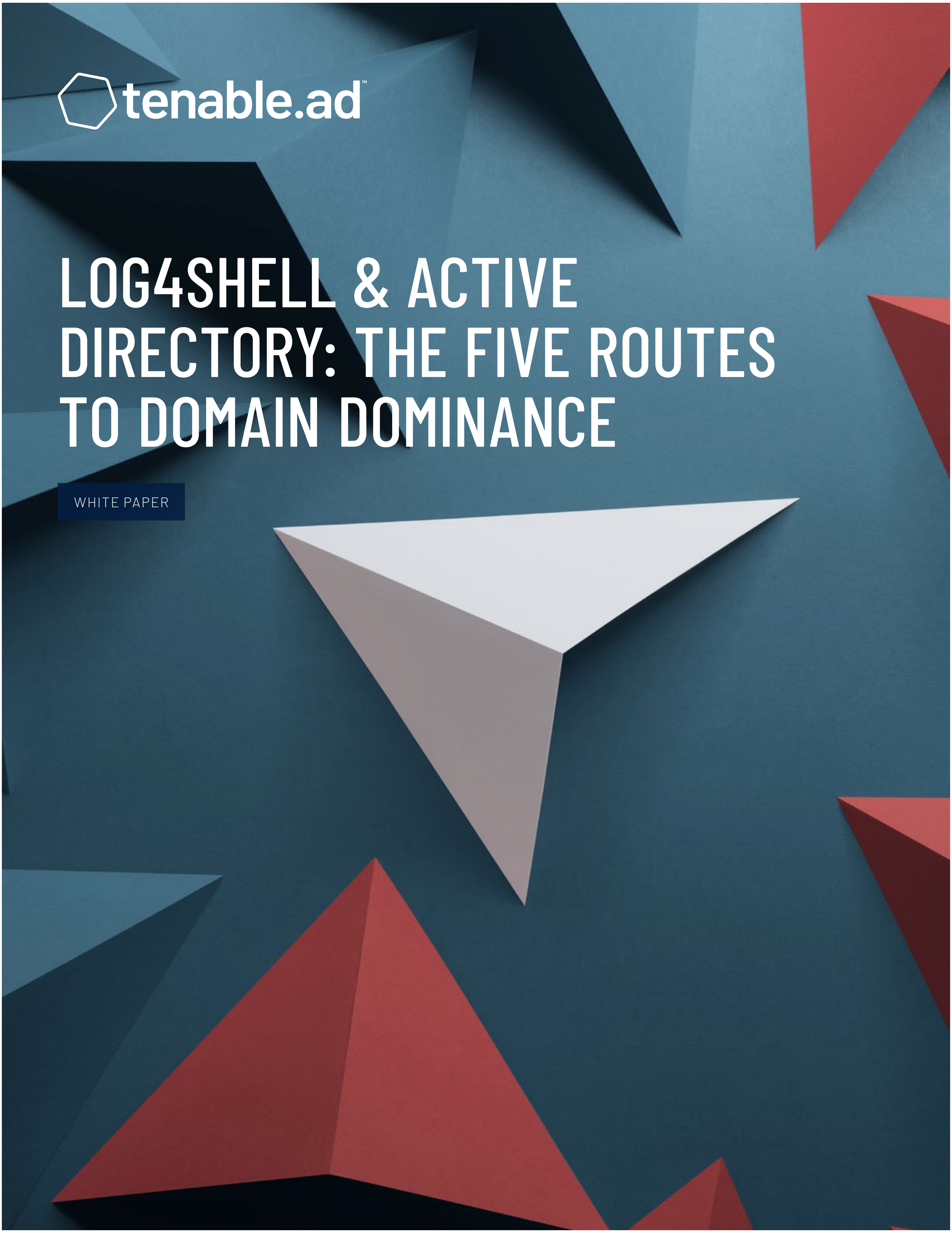
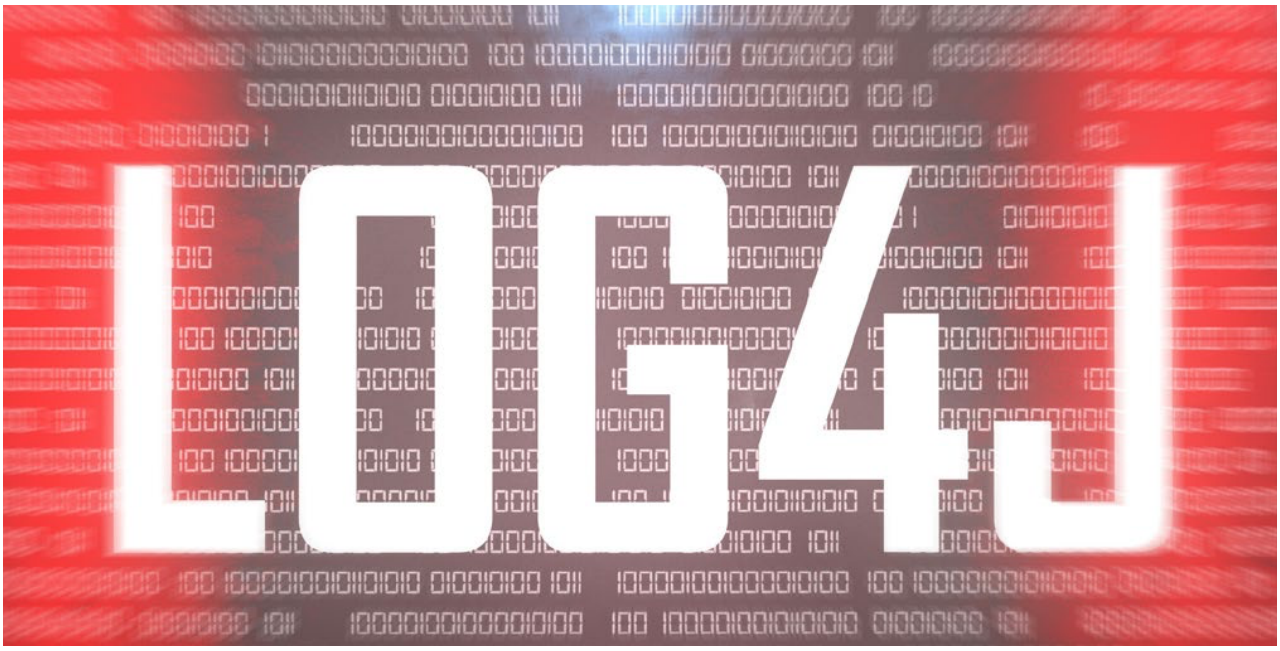


tenable.ad™

# LOG4SHELL & ACTIVE DIRECTORY: THE FIVE ROUTES TO DOMAIN DOMINANCE

WHITE PAPER



Whilst much has been written about Log4j and the potential impact to the applications that rely on the now infamous java library, little has been said about how attackers could leverage the flaw to gain control of your domain at the highest levels of privilege.

"But there is no Java in Active Directory" I hear you all cry...

## There is no Java in Active Directory

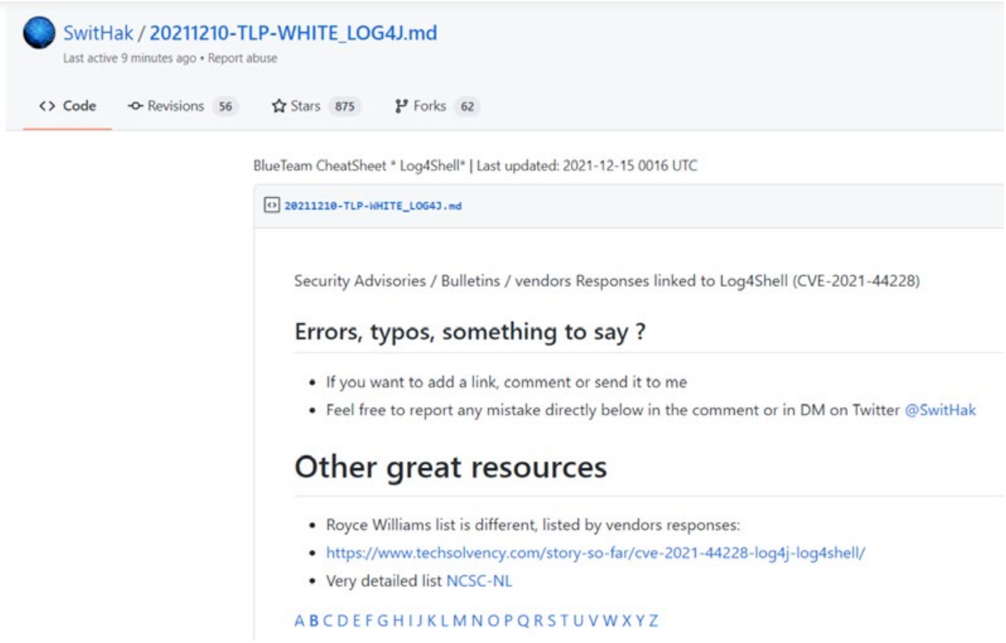
Sounds like good news, right? And it is, to a certain extent. Unfortunately, it's a little more complicated than that, and this flaw is a very tangible, albeit indirect, threat to most Active Directory infrastructures.

For the purpose of this article, we will assume that you are familiar with Active Directory and that you understand its strategic position for information systems.

We will discuss five major situations in which Log4Shell allow attackers to achieve complete domain domination over your Active Directory infrastructure. These five situations are not exhaustive and, beyond any doubt, there are many other compromise paths using similar concepts.

Numerous sources try to enumerate the software that are vulnerable to Log4Shell. And while these sources are not exhaustive, we are going to use what they have already listed to develop our risk scenarios.

One of the most current lists referencing the impacted editors and solutions can be found at the following address: https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592



SwitHak / 20211210-TLP-WHITE_LOG4J.md

Last active 9 minutes ago • Report abuse

BlueTeam CheatSheet * Log4Shell* | Last updated: 2021-12-15 0016 UTC

20211210-TLP-WHITE_LOG4J.md

Security Advisories / Bulletins / vendors Responses linked to Log4Shell (CVE-2021-44228)

Errors, typos, something to say ?

- If you want to add a link, comment or send it to me
- Feel free to report any mistake directly below in the comment or in DM on Twitter @SwitHak

Other great resources

- Royce Williams list is different, listed by vendors responses:
- https://www.techsolvency.com/story-so-far/cve-2021-44228-log4j-log4shell/
- Very detailed list NCSC-NL

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

– Source: https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

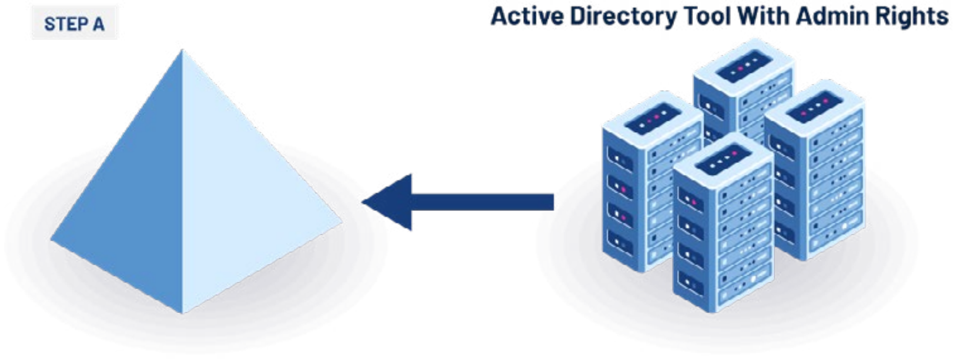
## Risk Situation #1

### Log4Shell-vulnerable AD management or security tools – IMPACT: DOMAIN DOMINANCE

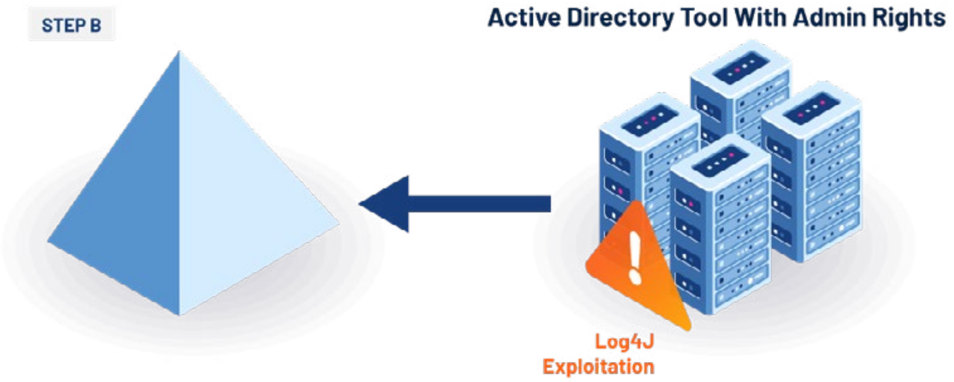
Numerous solution providers for Active Directory require a service account with elevated privileges. These elevated privileges on Active Directory mean these solutions have the ability to perform any action in the Active Directory database and in the SYSVOL directory.

If you are using one of these types of software, and if it is affected by the Log4J flaw, then anyone - anyone! - on your local network can take control of your Active Directory.

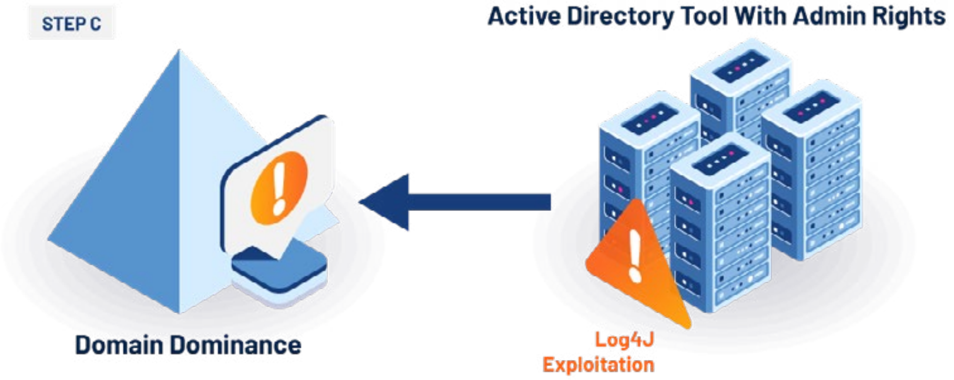
#### Step 1A: Using an Active Directory management or security software that requires elevated rights:



### Step 1B: The Log4Shell flaw is exploited on the Active Directory management or security software:



### Step 1C: Active Directory Domain Dominance



This is not a theoretical risk. A quick search will give you plenty of Active Directory management software affected by Log4J. If you use any of these solutions, then anyone on your local network can take control of your Active Directory domain.

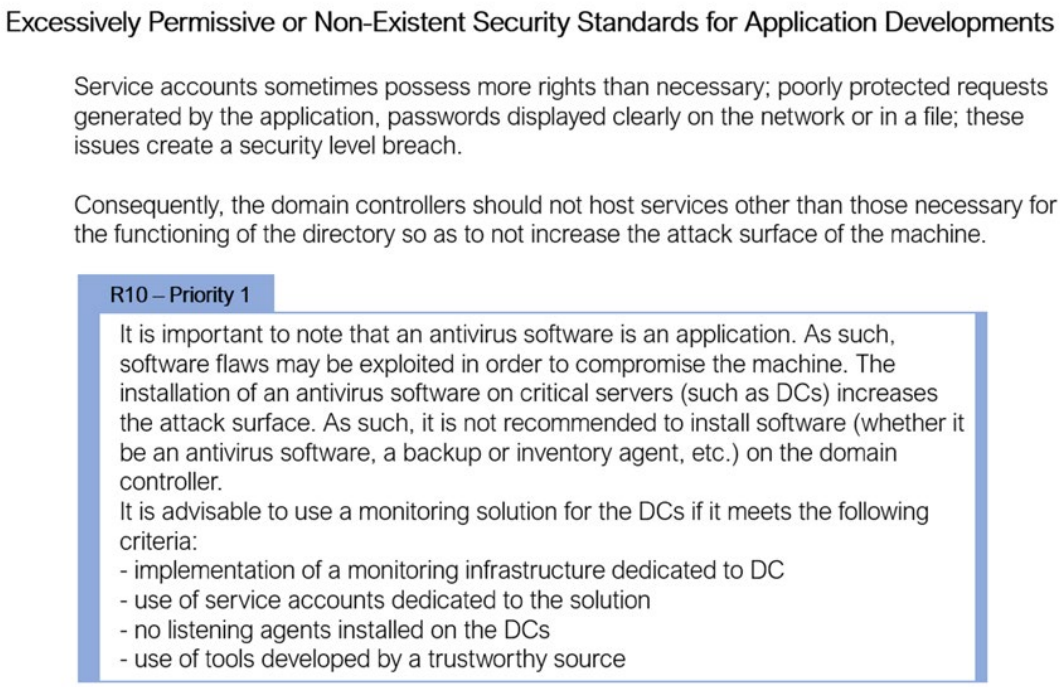
# Risk Situation #2

## Log4Shell-vulnerable AD management or security tools – IMPACT: DOMAIN DOMINANCE

Despite countless explicit recommendations from leading national cybersecurity agencies, numerous organizations continue to install anti-virus or EDR agents on their Active Directory domain controllers. This is a major mistake which leads to a dramatic increase of their attack surface.

If the EDR agents are installed on the domain controllers, and the agent is affected by this Log4Shell flaw, then anyone on your local network can take control of your Active Directory domain.

There's another way attackers can leverage EDR solutions to achieve the same results. Instead of using the vulnerability to compromise the EDR agents themselves, one may compromise a Log4Shell-vulnerable EDR management console instead. With complete control of the EDR management console, and with EDR agents installed on domain controllers, domain domination is a click away.



Excessively Permissive or Non-Existent Security Standards for Application Developments

Service accounts sometimes possess more rights than necessary; poorly protected requests generated by the application, passwords displayed clearly on the network or in a file; these issues create a security level breach.

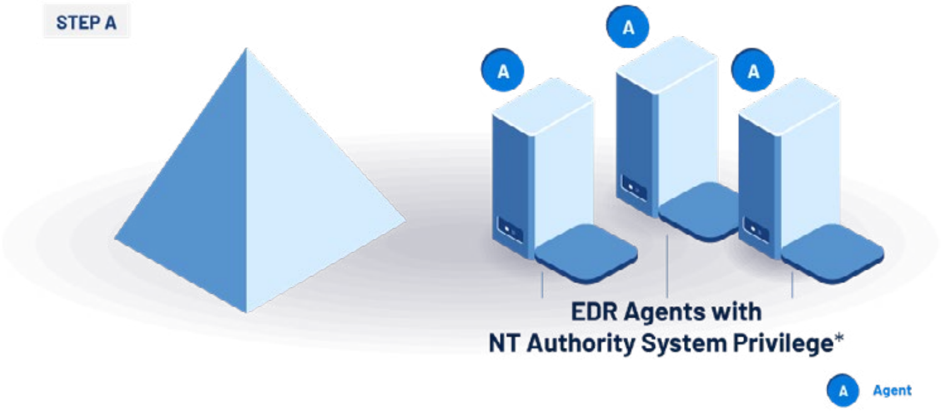
Consequently, the domain controllers should not host services other than those necessary for the functioning of the directory so as to not increase the attack surface of the machine.

R10 – Priority 1

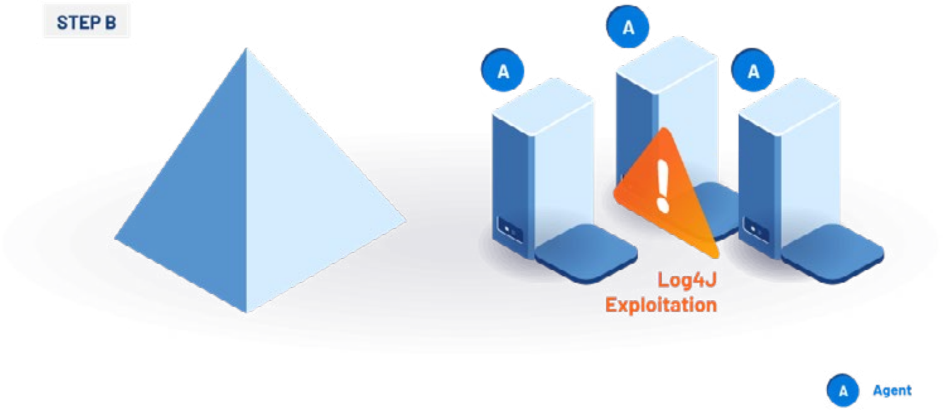
It is important to note that an antivirus software is an application. As such, software flaws may be exploited in order to compromise the machine. The installation of an antivirus software on critical servers (such as DCs) increases the attack surface. As such, it is not recommended to install software (whether it be an antivirus software, a backup or inventory agent, etc.) on the domain controller.
It is advisable to use a monitoring solution for the DCs if it meets the following criteria:
- implementation of a monitoring infrastructure dedicated to DC
- use of service accounts dedicated to the solution
- no listening agents installed on the DCs
- use of tools developed by a trustworthy source

– *Source: https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf*

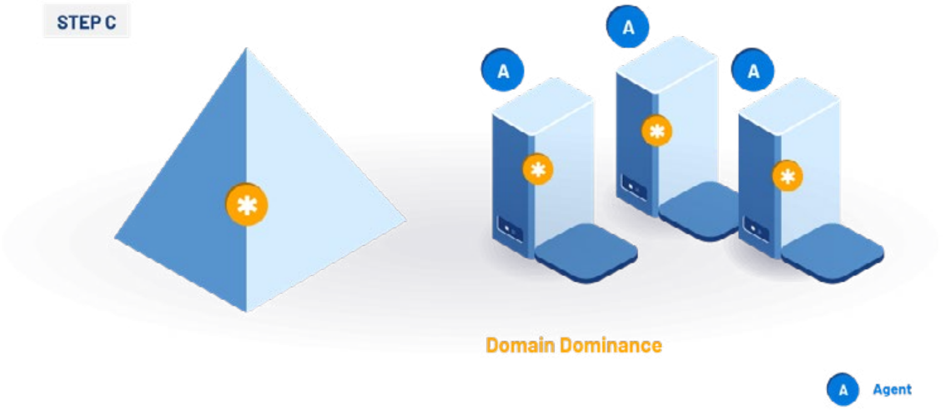
### Step 2A: Installing EDR agents on your domain controllers:



### Step 2B: Log4Shell is exploited against the EDR agents on an Active Directory domain controller:



### Step 2C: Active Directory Domain Dominance:



Again, many EDR providers have seen their on-prem management console affected by Log4Shell: if you are using such an EDR, anyone on your local network can take control of your Active Directory domain.

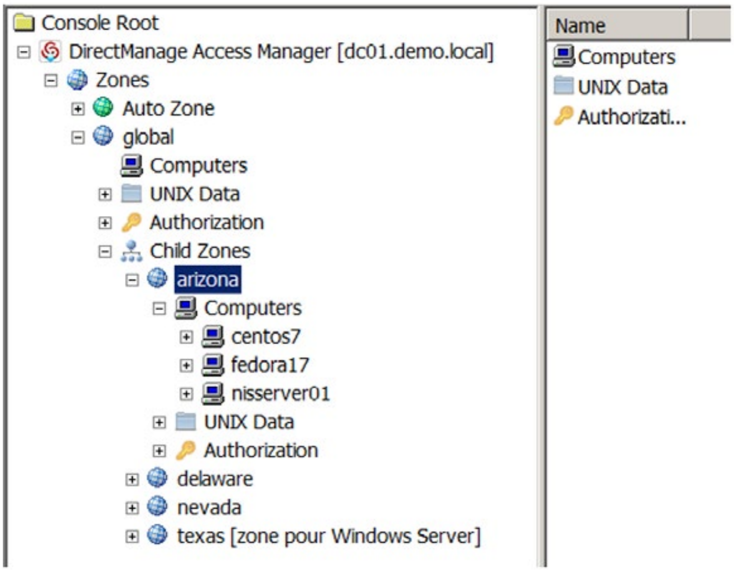
## Risk Situation #3

# Some Linux/UNIX systems are in “AD Bridging” status and host a Log4Shell-vulnerable application or demon – IMPACT: TIER-1 COMPROMISE

Active Directory bridging (AD Bridging) is a mechanism which allows users to connect to non-Windows systems (UNIX, Linux, MacOS) with Active Directory connection identifiers. This type of architecture enables system administrators to easily manage users, applications, data, and other aspects of their network by using a sole directory: Active Directory.

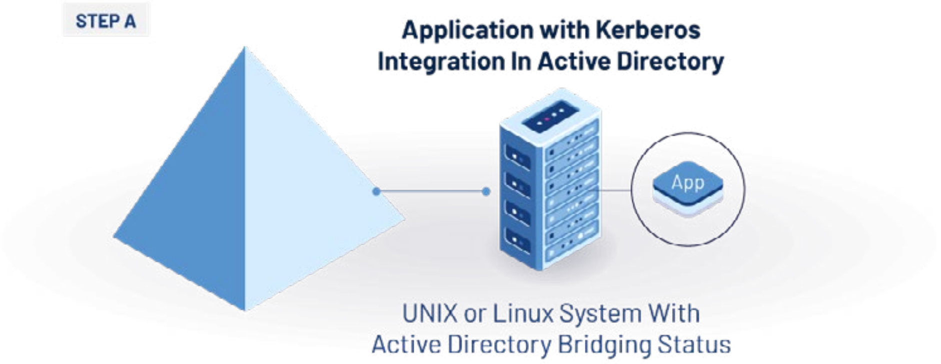
You can implement AD Bridging either by using the native functions of certain Linux distributions, or by using commercial products that allow for a wider functional covering. Note that Linux/UNIX server machines are generally considered as Tier-1 within the Microsoft Tiering model.

Management habits differ widely between UNIX and Windows production teams. None of them is good or bad, they are just different. One of these differences lies in the fact that, in an AD Bridging design, you need to have service accounts with the same password on a set of UNIX Tier-1 machines. And so if one of these UNIX machines gets compromised, then the attacker can escalate its local privilege and move laterally to all Tier-1 machines.

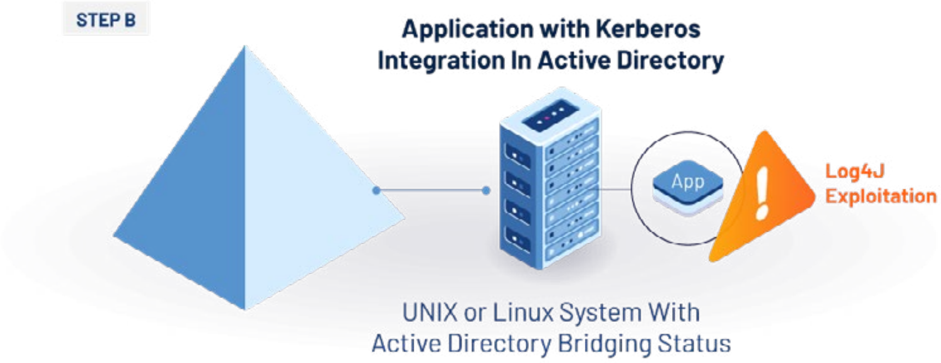


- [Source: https://www.identitycosmos.com/http:/www.identitycosmos.com/technique/unix_nis_maps_active-directory](https://www.identitycosmos.com/http:/www.identitycosmos.com/technique/unix_nis_maps_active-directory)

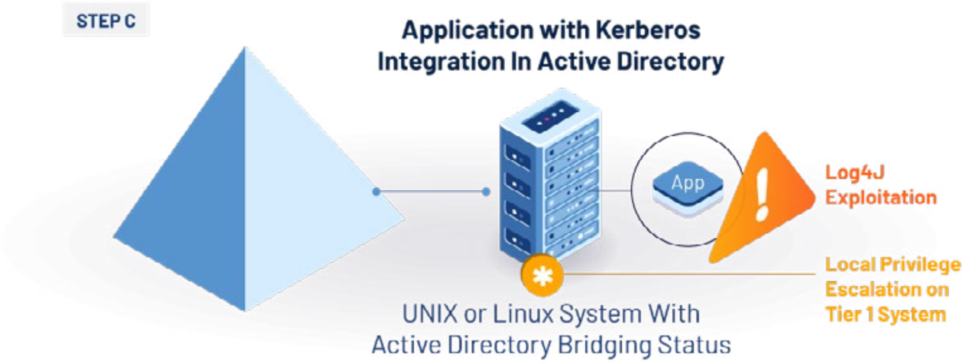
Step 3A: Implementing AD Bridging: A Unix system is integrated in Active Directory and hosts an application with Kerberos integration


STEP A
Application with Kerberos Integration In Active Directory
App
UNIX or Linux System With Active Directory Bridging Status

Step 3B: The Log4Shell flaw is exploited on the UNIX system or on the application with Kerberos integration:


STEP B
Application with Kerberos Integration In Active Directory
App
Log4J Exploitation
UNIX or Linux System With Active Directory Bridging Status

Step 3C: Compromise of the UNIX system, and probable lateral movement to all UNIX systems present on Tier-1.


STEP C
Application with Kerberos Integration In Active Directory
App
Log4J Exploitation
Local Privilege Escalation on Tier 1 System
UNIX or Linux System With Active Directory Bridging Status

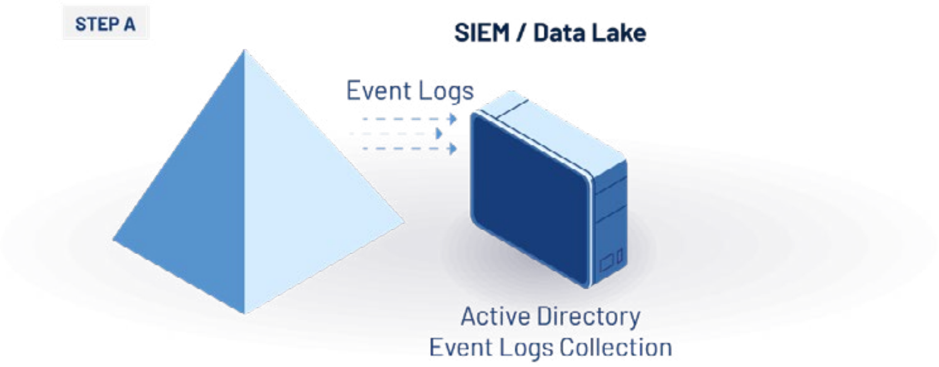
## Risk Situation #4

### Log4Shell-vulnerableSIEM or Data Lake solution – IMPACT: HIDING IN PLAIN SIGHT

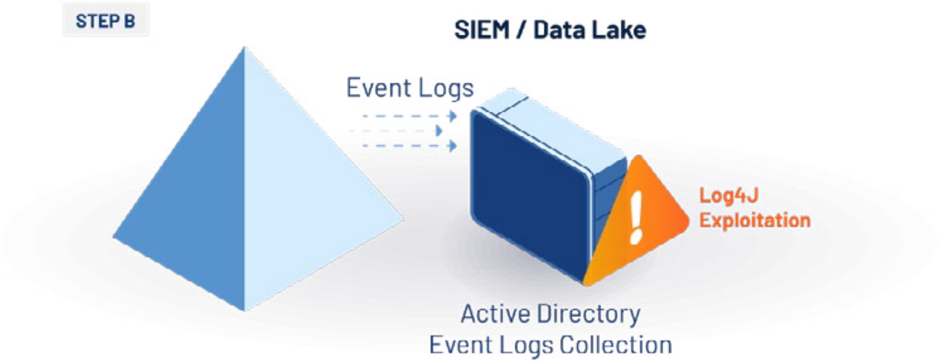
Many organizations use a SIEM and/or a Data Lake solution to collect, store, and correlate security events.

If a SIEM or Data Lake solution is vulnerable to Log4Shell, attackers can hide their actions within Active Directory by manipulating the collected data, or by changing the configuration of alerts within the SIEM.

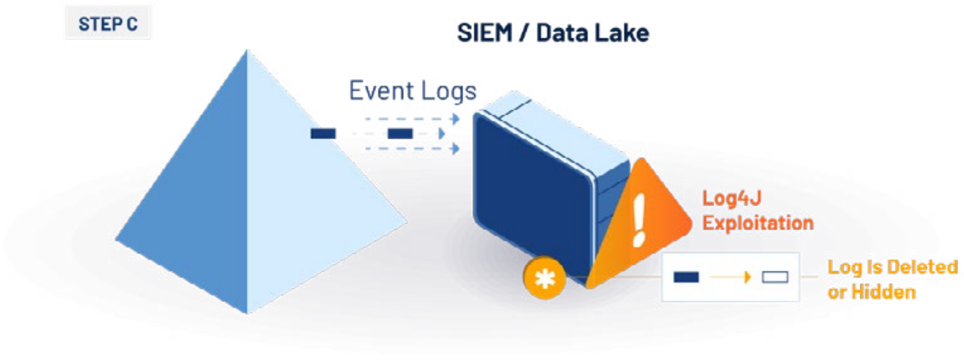
### Step 4A: Implementation of a SIEM with collection of events from the domain controllers



### Step 4B: The Log4Shell flaw is exploited on the SIEM.



### Step 4C: The attacker has the capacity to hide all its malicious actions created in Active Directory by deleting certain data in the SIEM, or by modifying the correlation or event alert rules.



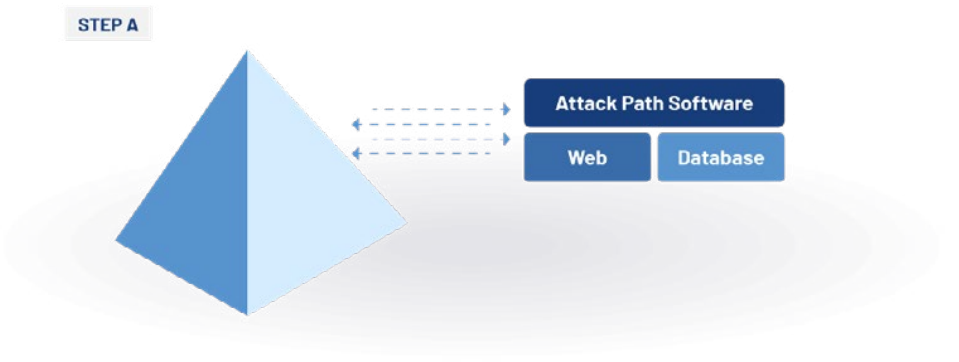
## Risk Situation #5

## Log4Shell-vulnerable AD paths visualization solution – IMPACT: BACKDOORS CONCEALMENT

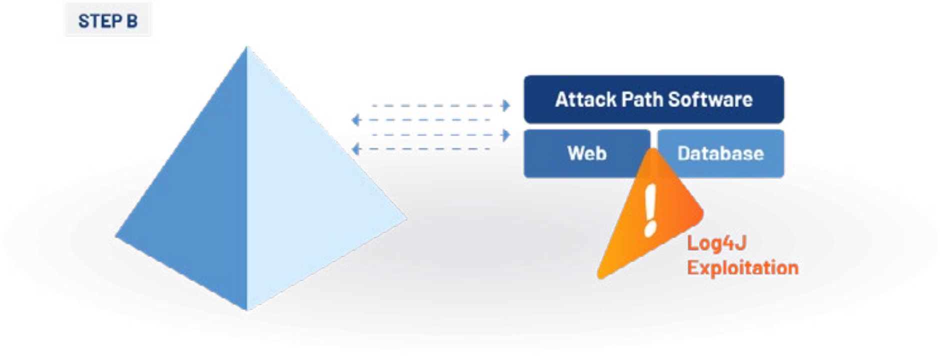
The Log4Shell flaw bears a particularity: it can affect a software itself, or just a component of it. This makes the inventory of the flaw extremely complex, since it requires organizations to have the ability to scan and audit all components, and not only the software "surface".

An illustration of this lies in some attack path visualization solutions that are based on open-source libraries affected by the Log4Shell flaw.

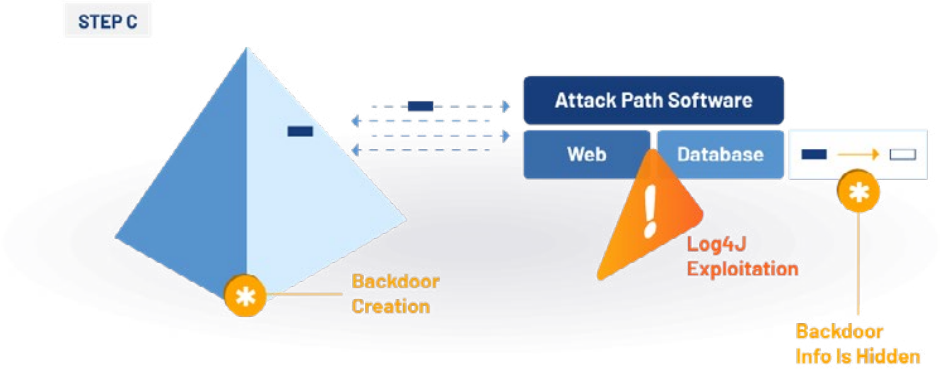
### Step 5A: Implementation of an attack path visualization solution with collection of information from the domain controllers.



### Step 5B: The Log4Shell flaw is exploited on one of the components of the Active Directory attack path visualization software.



### Step 5C: The attacker can now exploit Active Directory misconfigurations (typically in order to establish persistence through backdoors ) while hiding all its malicious actions from the attack path visualization tool's users.

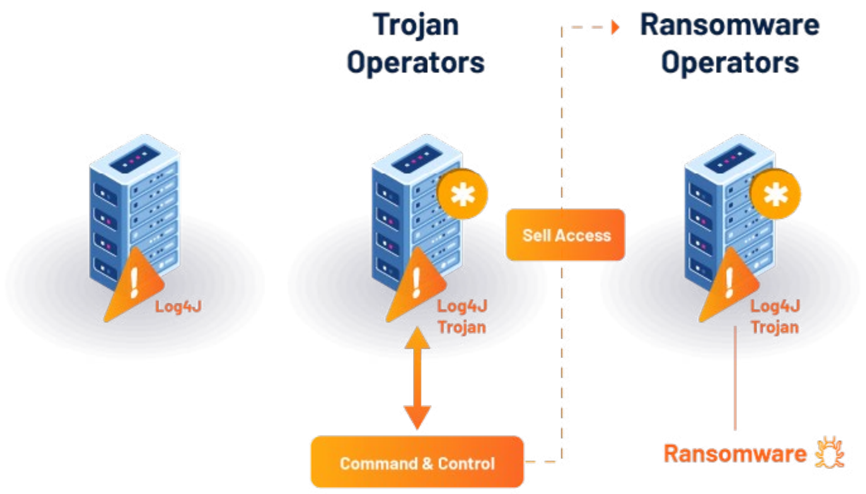


Most attack path / data visualization solutions use Neo4J to store AD data. As of the date of this article, Neo4J versions 4.2+ are impacted by the Log4Shell flaw. This example perfectly illustrates the importance of nested dependencies, notably in the Open-Source world.

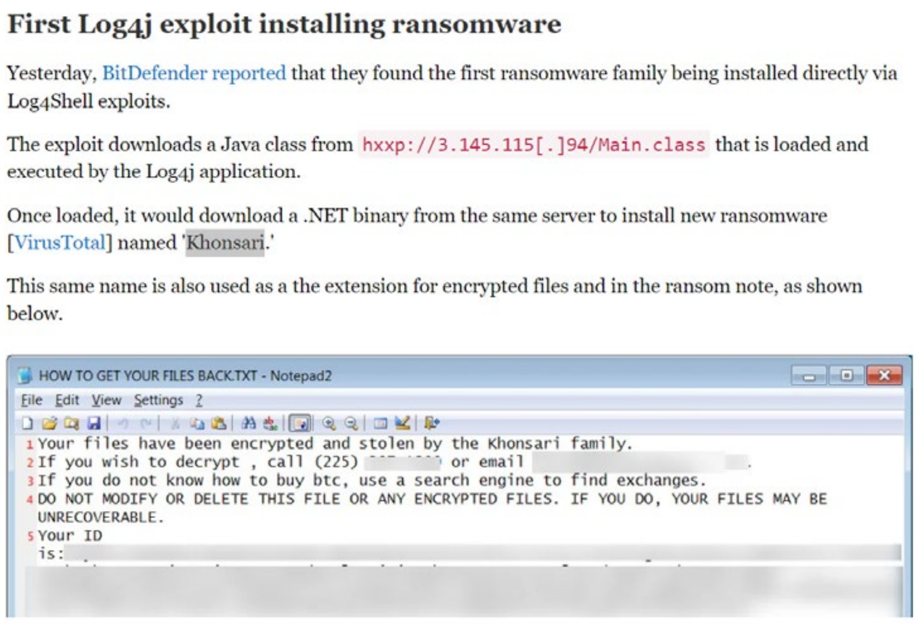
- *Source: https://community.neo4j.com/t/log4j-cve-mitigation-for-neo4j/48856*

# Is Log4Shell flaw exploitable by Ransomware operators?

Generally, new vulnerabilities are not immediately exploited by ransomware. Other operators though could be. For example threat actors reselling "primo-infections" and remote access in "Command & Control" mode via Trojans are the most likely to exploit new opportunities such as Log4Shell:



That being said, it turns out that Log4Shell has been actively exploited by a new breed of ransomware only 5 days after the vulnerability went public. This new ransomware - "Khonsari"- uses Log4Shell as a mean to deploy a network discovery tool, which will in turn deploy the encryption payload. A multi-stage approach that's typical of ransomwares.



## First Log4j exploit installing ransomware

Yesterday, BitDefender reported that they found the first ransomware family being installed directly via Log4Shell exploits.

The exploit downloads a Java class from `hxxp://3.145.115[.]94/Main.class` that is loaded and executed by the Log4j application.

Once loaded, it would download a .NET binary from the same server to install new ransomware [VirusTotal] named 'Khonsari.'

This same name is also used as a the extension for encrypted files and in the ransom note, as shown below.

HOW TO GET YOUR FILES BACK.TXT - Notepad2
File Edit View Settings ?

```
Your files have been encrypted and stolen by the Khonsari family.
If you wish to decrypt , call (225) [redacted] or email [redacted].
If you do not know how to buy btc, use a search engine to find exchanges.
DO NOT MODIFY OR DELETE THIS FILE OR ANY ENCRYPTED FILES. IF YOU DO, YOUR FILES MAY BE
UNRECOVERABLE.
Your ID
is: [redacted]
```

- Source: https://www.bleepingcomputer.com/news/security/new-ransomware-now-being-deployed-in-log4shell-attacks/

## Conclusion

If Active Directory is important to you - and we certainly hope it is - then it is urgent you expand your Log4J scanning and fixing efforts to all the types of solutions we highlighted in this document. All of them could grant direct or indirect control of your AD to attackers.

For additional information on Log4Shell, please read these articles on the Tenable website:

https://www.tenable.com/blog/apache-log4j-flaw-a-fukushima-moment-for-the-cybersecurity-industry

https://www.tenable.com/blog/apache-log4j-flaw-puts-third-party-software-in-the-spotlight

https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability

In order to secure your Active Directory infrastructure with an agent-free solution without elevated privileges, please check our website dedicated to tenable.ad: https://www.tenable.com/products/tenable-ad

Thank you for taking the time to read this article.
Sylvain Cortes – Security Strategist - Tenable

### About Tenable

Tenable, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

tenable.ad™