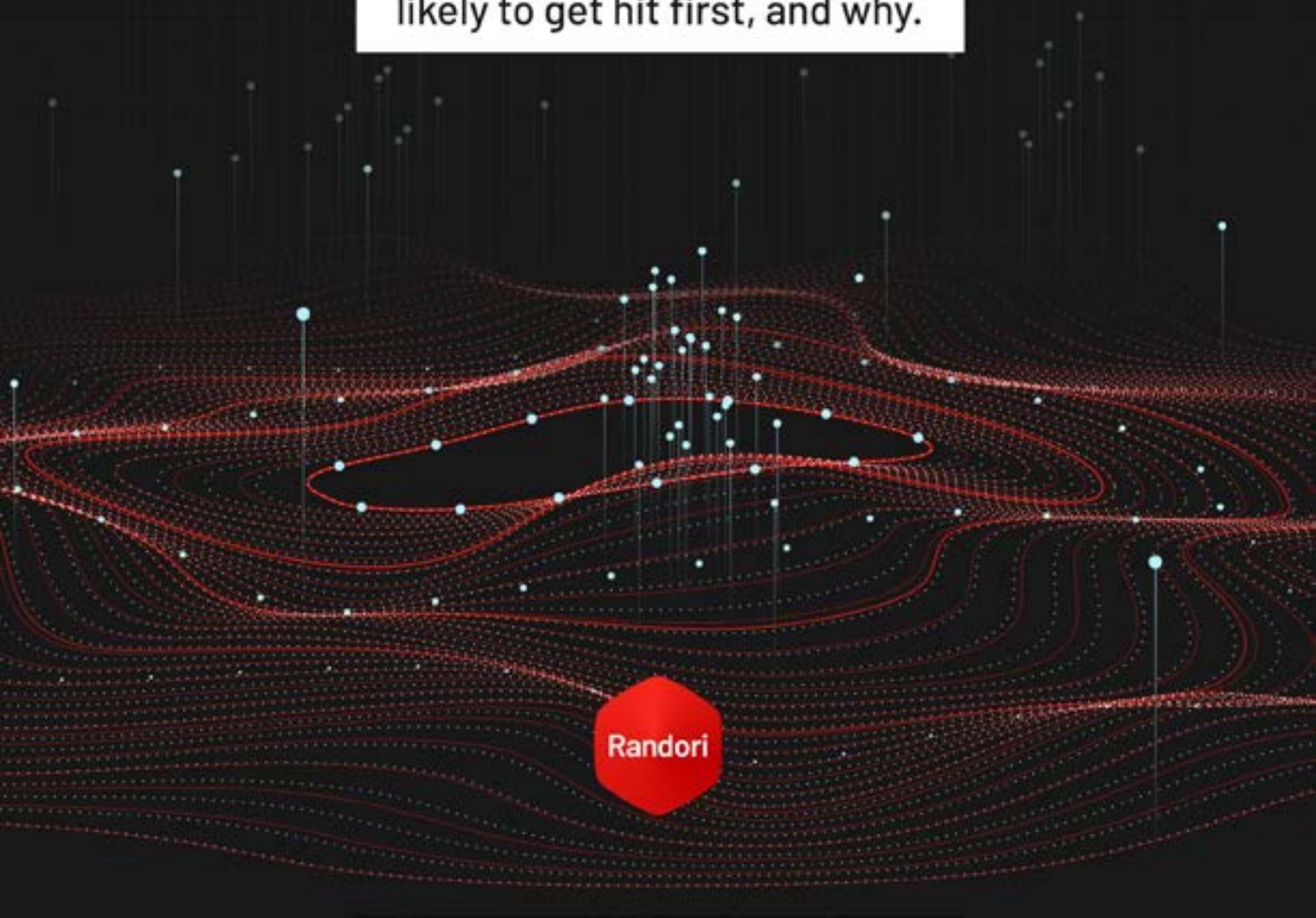
The Top Ten Most Attackable Log4j Applications

Randori 's guide into the most commonly exposed software using Log4j and the ones most likely to get hit first, and why.



Introduction

Log4j took the security community by storm in December 2021. It's widely used and, if unpatched, extremely easy to exploit, putting it high on any adversary's list. Cybersecurity experts agree it's the worst security flaw they've seen exposed in decades. The industry rallied as fast as it could to apply patches and remediation strategies, but undoubtedly vulnerable code still runs and is part of many established software platforms. Log4j attacks will continue for months, if not years to come. There are many reporting that VMware Horizon servers are under active exploitation by many criminal groups.

Seeing a gap in the market in knowing the riskiest applications affected by Log4j, Randori is unveiling research that identifies the most internet-exposed, widespread software affected by Log4j. Not all software utilizing Log4j is equally attractive from an attacker's point of view, so we'll unpack which software targets are actually most tempting and how attackers decide what to go after. We're in the unique position of continuously evaluating the attack surface of hundreds of companies, and layering on our attacker's perspective, we can identify the most attackable Log4j affected software visible on the internet.

Top 10 Most "Widespread" Applications Using Log4j Exposed on the Internet	Top 10 Most "Attackable" Applications Using Log4j Exposed on the Internet
1 cPanel	1 VMware Horizon
2 Apache Tomcat	2 Jamf
3 VMware Horizon	3 MobileIron
4 Eclipse Jetty	4 Ping Identity's PingFederate
5 IBM WebSphere DataPower	5 Jenkins
6 Eclipse JSP	6 Avaya IP Office
7 Atlassian Jira	7 SAP NetWeaver
8 PingFederate	8 Atlassian Confluence
9 Atlassian Confluence	9 Atlassian Jira
10 Jamf	10 cPanel

UNDERSTANDING THE LISTS

The "most widespread" list examines the most prevalent Log4j affected applications that are internet facing. This ranking is based on the volume of affected software, both in the number of instances at an organization and the number of organizations that have that technology running.

This list should remind organizations that if you use any of these services to check **every instance of it that's visible on your attack surface to ensure it's not vulnerable.**

The "most attackable" list takes into account other factors an adversary would consider before attempting exploitation. **The Most Attackable list better reflects risk and where initial damage would likely occur** because it goes beyond prevalence to consider:

- How important is software to the business? If an attacker exploits it, will it give them privileged access?
- How hospitable is the asset once a bad actor is on the inside? Will there be security software on the asset that could detect them? Assets that don't have a lot of security software are much more interesting and tempting to an attacker.

Widespread vs. Attackable: Which Top Ten List Is More Useful to Understand Risk?

> **"The most intriguing types of software from an attackers' perspective are those that are 100% confirmed to be vulnerable to Log4j and provide additional "downstream" access."**

Applications that provide authentication, automation, and configuration mechanisms present excellent opportunities for an attacker to pivot and expand operations inside an organization's network. Most of the widespread software are app servers or middleware—cPanel, Tomcat, Jetty, JSP, Wildfly—which are not 100% confirmed to use a vulnerable version of Log4j, making them a less interesting target to an attacker. These types of services may use optional components that use Log4j, and might come in a variety of configurations which can complicate locating an exploitable mechanism, so an attacker may not want to waste his time (especially if there is an easier target).

While prevalence is an important factor weighed by an attacker, it's not the only thing.

Just because there is a high volume, doesn't mean it presents the greatest risk to a business.

To get at the attackability of a service, attackers also consider the criticality of the application to the business. This includes factors such as whether or not the application will be hospitable to them once exploited (known as the post exploitation environment), and what other components will be accessible (known as reachable surface area) once hacked.

With that in mind, VMware Horizon, Jamf, and PingFederate become more tempting despite their lower prevalence.

And among those, software that is more widespread and gives great access reach the very top of the attacker's list, and so rank high on attackability. These applications were 100% confirmed to be vulnerable to Log4j and can potentially give instant privileged access. They provide a "one and done" scenario. For a business, these services—if not properly segmented or monitored—present the highest risk if compromised.

Let's take a deep dive into the most tempting Log4j affected targets.

Case Study: Stopping Log4j Without a Patch

Most, if not all Randori customers were vulnerable to the Log4j bug, however, two-thirds of our customers were able to stop us from successfully exploiting the vulnerability. Specifically, they were successful at blocking exfiltration, and prevented exploitation. By blocking outbound traffic on internet-facing apps, we were not able to exfiltrate any data.

Turning off outbound communications for all mission-critical applications, especially internet-facing apps—like VPN, network monitoring, device management or configuration tools can be what stops an attacker from successfully completing their objective.

What set these organizations apart:

- Proactive monitoring
- Strong segmentation
- Default deny

Top 10 Most Attackable Applications Using Log4j Exposed on the Internet

LEGEND:

Totally going pwn it, game over.

A bit more work, but worth it.

If there isn't an easier way in.

1 VMware Horizon

WHAT IS IT?

VMware Horizon is a virtual desktop infrastructure capability.

HOW COMMON IS IT?

Very common, approximately 10% of enterprises have VMWare Horizon exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

Within hours of Log4j being publically disclosed, Randori was able to prove that VMWare Horizon was vulnerable and could be exploited. As an attacker, if you control the virtualization platform, you can potentially influence any of the endpoints or infra running inside that virtualization capability. Further, it appears as many as 10% of large enterprises have VMware Horizon exposed to the internet - making it all the more tempting. VMware issued a patch soon after Randori alerted them to the vulnerability, but that doesn't mean everyone has patched their Horizon instances. In fact, Microsoft reported seeing exploitation in the wild.

2 Jamf

WHAT IS IT?

Jamf provides a platform to configure and automate IT administration tasks for macOS, iOS, iPadOS, and tvOS devices.

HOW COMMON IS IT?

Common, approximately 2% of enterprises have Jamf exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

Jamf was proven to be exploitable hours after Log4j was disclosed. Compromising Jamf could be a game-over event for an organization. If an attacker can control the configuration automation platform, he can influence any device that is being administered by that platform. This would make an ideal pivot and expansion platform for an attacker. Our attack team put this high on the list when Log4j came out initially (in fact, we confirmed exploitability on Dec. 10), but would deprioritize after Jamf released their updates.

3 MobileIron Mobile Device Management

WHAT IS IT?

MobileIron is a mobile device, application, and content management platform.

HOW COMMON IS IT?

Common, approximately 1% of enterprises have MobileIron exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

If an attacker can control a device management solution—just like Jamf— they can likely pivot and expand to other enterprise components. With Log4j things moved so quickly that within five days of discovery, NCC Group warned people that they had already seen five instances of active exploitation of MobileIron via Log4j.

4 Ping Identity's PingFederate

WHAT IS IT?

PingFederate is an enterprise federation server that enables user authentication and single sign-on.

HOW COMMON IS IT?

Common, approximately 2% of enterprises have PingFederated exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

PingFederate was confirmed to be affected by Log4j, boosting its temptation score. Thankfully they've issued releases that permanently resolve the issue. If an adversary can control the AUTH server and process, they can likely impact many other services that are serviced by that authentication mechanism. This becomes even more interesting if the way it's configured enables the attacker to create users in your environment.

5 Jenkins

WHAT IS IT?

Jenkins is an open source automation server that enables developers to build, test, and deploy their software.

HOW COMMON IS IT?

Common, approximately 1% of enterprises have Jenkins exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

Jenkins does not contain Log4j dependencies in its core; however, because it is itself a Java application, it is frequently used with plugins that consume Log4j. Jenkins is very interesting because it is frequently used for automation, which can lead to the "keys to the kingdom". If you can control the automation server, you can control the things being automated, including the source code.

6 Avaya's IP Office

WHAT IS IT?

IP Office is an on-prem or cloud-based VoIP + voice mail, speech to text, call forwarding, etc. for apps and physical Avaya devices.

HOW COMMON IS IT?

Not very common, less than 1% of enterprises have Avaya IP Office exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

The phones weren't necessarily vulnerable, but the management system was, and an outage could severely affect an organization, not to mention hard to remediate. And, as an adversary, being able to inspect the communications of a target is hugely beneficial—especially for nation-state-level adversaries.

7 SAP's NetWeaver

WHAT IS IT?

NetWeaver is a Java application server that uses the Log4j library for basic logging.

HOW COMMON IS IT?

Common, approximately 2.5% of enterprises have SAP NetWeaver exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

Application servers are particularly concerning because each Java application could also be independently leveraging Log4j functionality, requiring security teams to inspect each individual app running in the app server for vulnerable usage. In the case of NetWeaver, our attack team couldn't 100% confirm it's vulnerable (the details are behind a customer portal), but made the assumption it's vulnerable because SAP provided mitigating steps.

8 9 Atlassian's Confluence and Jira

WHAT IS IT?

Jira and Confluence help teams manage work and be more efficient and productive.

HOW COMMON IS IT?

Common, approximately 3% of enterprises have Jira or Confluence exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

Jira and Confluence fall into the "don't use Log4j" by default because Atlassian chose to fork a version of Log4j at some point in the past. There are articles that describe how to configure the two services to use vulnerable versions of Log4j, so we included them as items of interest for our customers. From the attacker's perspective Jira and Confluence most likely won't give privileged access, and it is unlikely that very many instances are configured in a way that would leave them vulnerable, but they are great places to mine for information to use to pivot, or exploit something else.

10 cPanel

WHAT IS IT?

cPanel is a web-hosting control platform with a Linux-based GUI.

HOW COMMON IS IT?

Extremely common, approximately 37% of enterprises have cPanel exposed on their attack surface.

WHY IS IT TEMPTING TO AN ATTACKER?

cPanel is the most prevalent Log4j affected software and the sheer volume of it was staggering—37% of organizations have multiple instances of cPanel visible on the internet. While the core of cPanel is not vulnerable, the cPanel ecosystem has many optional components that do use Log4j, like Apache Solf (search functions) and Dovecot (IMAP and SMTP email functions). This reinforces the point that organizations need to understand the whole stack of software that underlies their platforms. The dependencies of large enterprise software deployments are frequently opaque, and hard for the administrator looking for bugs to know what's under the hood.

Where We Are Today

Defenders are going to be dealing with Log4j for a while. Sadly, the industry can't completely write off Log4j because of the nature of its use. It's buried deep into layers and layers of shared third-party code, and defenders have to go spelunking into proprietary software to see if it's using Log4j. Or if they are using cPanel, TomCat, Jetty, JSP, or any other software that has Log4j components, further investigation is required. ***Adding in the attacker's perspective is critical to understanding your real-world risk***. By doing this, you immediately get to what's most critical to fix first, and then you can branch out to fix lower risk services.

In the early days of Log4j one would expect attackers to throw experimental exploits against everything because "good" targeting information was hard to come by. ***At this point in the Log4j vulnerability lifecycle, more sophisticated adversaries will perform much more targeted attacks—seeking out those who are still using unpatched versions of exploitable software.*** We're already seeing this play out: Horizon is being used in the wild, as is Jamf and others. Less sophisticated adversaries are playing the "spray and pray" game, using it with ransomware campaigns.

The good news is that there are actions defenders can take today to mitigate Log4j harm on a broader scale. Proof: ***two-thirds of Randori customers successfully blocked callbacks and prevented exploitation before patches were available. We landed on their machines, but we were not able to get out with any data because these customers successfully blocked exfiltration and prevented exploitation. By simply blocking outbound traffic on internet-facing apps we were stopped from directly executing code on these targets.***

For defenders, actions may seem futile, but as we continue to plug away at identifying vulnerable versions of Log4j, we need to put more of an emphasis on making systems more resilient, and less on catching and patching bugs. Log4j isn't the first, and it won't be the last. In lieu of a catch-all solution, we need to ensure we not only patch, but invest ways to make our systems more secure.

Tips for Defenders To Curb Log4j Incidents

01

Review your attack surface to enumerate any external-facing devices that have Log4j installed. Randori can help with this. We'll give you a free Log4j Perimeter Report to help jump-start your program.

02

Ensure that your security operations center (SOC) is actioning every single alert on the software and services that are known to contain Log4j.

03

Install a web application firewall (WAF) with rules that automatically update so that your SOC is able to concentrate on fewer alerts, such as Google Cloud Armor.

04

Turn off outbound communications for all your mission-critical applications, especially internet-facing apps—like your VPN, network monitoring, device management or configuration tools.

What to Learn More About Protecting Your Attack Surface?

If you found this data helpful, you may also be interested in securing a free Randori Recon report to discover what's exposed on your attack surface and learn more about the tempting targets on your perimeter.

CONTACT US FOR A FREE ATTACK SURFACE REVIEW →

Other resources you may like include:

2021 Randori Attack Surface Management Report

The CISO's guide to identifying the most attackable assets on their attack surface. This report gives defenders a closer look at the software an attacker is most likely to go after and target for exploitation found on an attack surface.

DOWNLOAD →

SANS Guide to Evaluating Attack Surface Management

ASM is an emerging security category that aims to help organizations address the expanding risk posed by cloud computing and the rapid transition to work from home. Read this guide to learn how to evaluate the effectiveness of an ASM tool.

DOWNLOAD →

2021 Gartner Cool Vendor in Security Operations

Gartner estimates that a third of successful attacks experienced by enterprises will result from unknown shadow IT risks. Shadow IT isn't a new problem. Learn how to discover, prioritize, and remediate shadow IT.

DOWNLOAD →

About Randori

Randori attacks to protect. Recognized by Gartner & IDC as a leader in offensive security, the Randori Platform unifies Attack Surface Management (ASM) and Continuous Automated Red Teaming (CART) to provide enterprises the visibility, actionable insights, and validation they need to proactively prevent breaches. Customers like VMware, Greenhill Inc, FirstBank, NOV, Lionbridge, and many more, trust the Randori platform, xx` was designed by the world's foremost offensive security practitioners at nation-state levels.

Connect with Randori to discover what's exposed on your attack surface and learn more about the tempting targets on your perimeter.

LEARN MORE →