Securing your Backups Against Log4j Vulnerabilities

asigra


A Worrying New Variant/Vulnerability Emerges

Late November 2021 was a bad month for both pandemic response officials and security personnel alike. On the pandemic front, a newly identified variant of COVID-19, called Omicron, spread rapidly worldwide, becoming the most infectious viral disease in known history.

At the same time, a critical vulnerability identified in a common Java utility affects almost every major software vendor, application, cloud service, and connected device. That vulnerability, of course, is Log4j. Like the Omicron variant, its impact is measured in how widespread it is. Unlike Omicron, it's also incredibly severe, allowing cybercriminals to execute remote code on affected systems. The door is wide open for hackers to take remote control, install malicious software, download data or install ransomware. It's like the mythical "Deltacron" variant – as widespread as Omicron and as severe as Delta. Unsurprisingly, it's categorized as a 10/10 on the CSCC severity scale, requiring immediate action and response.

Why is Log4j a Ransomware Threat?

Imagine for a moment that you come back from a 2-week vacation and discover that you lost your keys. The last time you remember having them was when you locked the front door of your house and possibly left the keys in the door. So you do the responsible thing and get your locks changed. If someone took your keys, what have they been doing with access to your house for the last two weeks? Have they stolen anything? Put in cameras? Unlocked a basement window so they can break in again in the future? That's what security professionals are worried about with the Log4j vulnerability.

As a zero-day vulnerability, the Log4j issue was likely known to hackers for many weeks before cybersecurity experts knew its existence and could create patches for it. Even with Log4j patched today, the possibility that hackers have already implanted malware in affected systems is very high. Every organization that used the Log4j utility or any software that used the utility has exposed their systems to future ransomware attacks.

Log4j Mitigation Recommendations

Every organization has had to develop a mitigation plan, leading to a long and painful holiday for many IT administrators and security professionals. Your mitigation strategy has likely included scanning your environment to get a thorough inventory of every service or device using Log4j, patching said devices, and blocking outgoing requests to firewalls to minimize the ability of hackers to compromise your environment. But have you closely considered your backups?

Protecting Your Backup Environment

In addition to mitigating a large amount of your IT environment, critical attention must be paid to your backup environment, particularly when it comes to ransomware threats. Backup systems are a significant target for ransomware. If attackers can compromise your backups or your backup software, they will be more successful at extorting your company to get your data back.

Beware of Attack-Loops™

Ransomware attackers have been heavily focusing on backups because they know a good backup thwarts their payday. They've been modifying their tactics, focusing on implanting dormant ransomware weeks and months before an attack. When you recover your systems, you recover the ransomware simultaneously, creating an Attack-Loop.

In addition to this, they are using credential hunting to get direct access to your backup systems so that they can delete or corrupt sets or change retention policies on "temporary immutable" data sets.

Besides being a terrible year for ransomware attacks (2021 saw 100% growth in the number of cyberattacks), 2022 shows an exponential increase in hacker attacks due to the Log4j vulnerabilities.

Even as early as December 14th, over 840,000 attacks had already occurred. And there are several known ransomware packages (Khonsari, Night Sky) using the Log4j vulnerability to attack vulnerable systems.

You May Already Be Compromised

The most worrying aspect is that this vulnerability may already have compromised your backup software. (Asigra does not use JNDI and is not susceptible to Log4j). Backup agents are also vectors. (Asigra doesn't use agents) If your backup software is vulnerable, you'll need to upgrade your backup systems and every system that uses a backup agent if you haven't already. It's a heavy administrative burden but necessary given the threat severity.

Other systems are at risk. Given the time frame that the exposure was known and the complexity in getting patches from vendors, you may have already been exposed to ransomware prior to updating and patching systems, as ransomware groups moved very quickly to take advantage of the vulnerability. It's recommended that you take the following measures in regards to your backups:

1. Start scanning all existing backup data sets for any known malware or ransomware, including any new ransomware variants created to take advantage of Log4j vulnerabilities.
   a. **Note:** Asigra has inline backup and recovery malware scanning, using an AI engine & machine learning to detect known malware signatures & identify behavior heuristics to identify zero-day attacks, both when data is backed up and prior to you recovering your data.
2. Quarantine any suspect backups.
3. Scan existing live data sets for malware, and recover data from known clean backups.
4. Rebackup any compromised backup sets from known clean live systems.

Long-Term Log4j Innoculation

Log4j may be a long-term threat as vendors and software developers alike go through their systems to identify the use of this logging tool and validate what versions they have. Several hardware devices and IoT devices, even printers, need to be updated. And you may have WFH users who are using their systems and devices on your network.

Note that Log4j will not be the last major vulnerability. There will be more. (Additional vulnerabilities were found in Log4j soon after the initial one). Some of those will be zero-day attacks where the hackers discover the vulnerability, and there is no patch to protect you. The likelihood of this occurring is so high that you should be operating as if it already is.

You can take preventative measures to protect your backup data and prevent yourself from being a ransomware target from this, or other future discovered vulnerabilities.

Use Agentless Backup Software

There has long been a debate in backup software circles over the advantages and disadvantages of using agentless backup software. On the plus side, there's a huge reduction in management – no agents to deploy or update. On the other hand, they tend to increase network traffic as some pre-processing tasks are not done on the client-side. Those disadvantages can be minimized with compression software and incremental forever backup features.

The Log4j vulnerability should finally put this debate to rest. No backup software should have agents installed on client systems. This vulnerability has shown just how dangerous it is to have an extra potential security hole open on all of your servers and endpoint devices. If only one of those remains unpatched, you have an open door for hackers to attack you.

Asigra Tigris Ultra Secure Backu is one of the only enterprise backup services that is agentless. There is no additional code or libraries that need to be installed on any servers or endpoint devices.

Air-gapped, Immutable Backups are not Good Enough

While Immutable backups are touted as the best option for ransomware protection, they can provide you with a false sense of security. (See Tech Data's Article on immutability drawbacks)

Criminals are actively hunting for credentials, and if they get access to your backup systems, they can wreak all kinds of havoc. They can insert ransomware as sleeperware, which causes your infected data to become "immutable" when backed up, even if it's air-gapped. They can also change your temporary immutable data retention policies and make other changes that prevent your backup sets from being fully recoverable.

Even immutable data can be stolen. The current trends are not just to encrypt data but to threaten to release it if a ransom isn't paid. This most likely happened to CD Projekt Red, which resulted in releasing their source code and other sensitive data. It would be best if you prevented backups from being compromised in the first place.

Filling the Gaps in Air-gapped & Immutability

Asigra solves this in three important ways.

1

Bidirectional Malware Scanning– Our software uses an advanced malware engine that is able to detect malware code signatures and behavior to find known and zero-day threats. Every backup is scanned, and suspect files are quarantined before backups are committed. In the event that an infected file still got backed up, the system also scans files before they are restored. And if ransomware is discovered during a restore, those files are quarantined, allowing you to restore as many of your clean files as possible.

2

Backup Encryption–Within the Asigra platform, your customers' data is protected at all times with the highest levels of security and compliance:

- AES 256-bit in-flight and at-rest data encryption
- Government-approved NIST FIPS 140-2 security certification
- Multi-factor authentication (MFA)
- Alternating Repository Naming creates a moving target for malware payloads
- Soft Delete provides a hidden/secret deletion folder for a set period of time

3

Deep MFA– Multi-factor authentication is the first step to prevent credential hunting attacks. MFA itself can be bypassed in some attacks, which is why we embed MFA deep into specific sensitive tasks, and those MFA requests can be routed to separate personnel. If someone is trying to delete a backup, the request will not go through until approved by the appropriate designated staff member.

Conclusion

Log4j is the most significant threat to your organization's data security. So far. According to many analysts, the number of ransomware attacks is predicted to continue to increase, and your backups are a prime target. With Asigra, you can better protect your backup environment in these uncertain times.

What's next?

Are you looking to strengthen your data security?
Learn more about Asigra Tigris Ultra Secure Backup.

Contact Us