Asigra Cyber-Secure Backup Platform Defending Data Against Persistent Log4j Vulnerability

Long Term Data Security Threat Mitigation Plans for Fast Remediation Include Protected Backup Environments that Ensure Recovery

TORONTO, ONTARIO, CANADA, March 8, 2022 /EINPresswire.com/ -- Asigra Inc., a leader in cyber-secure backup and recovery, today emphasized the requirement for protected backup environments to maintain business operations after an exploit of the Log4j vulnerability. Using a highly effective obfuscation tactic, the vulnerability allows malicious actors to conduct remote code attacks to expose/access sensitive data across IT domains. The effect of these exploits can be addressed in part with an effective data recovery strategy and solution as illustrated by the Asigra cyber-secure backup platform.

Discovered in Apache's Log4J, a logging system in widespread use by web and server application developers, the vulnerability makes it possible to inject text into log messages or log message parameters, then into server logs which can then load code from a remote server for malicious use. With the highest possible severity rating of 10 out of 10, security professionals are investing significant time and resources into countering this threat.

Organizations globally have been tasked with developing an effective Log4j mitigation strategy, which often includes infrastructure-wide scanning to get a thorough inventory of every service, server, workstation and client system using Log4J. This is followed by device patching and blocking outgoing requests to firewalls to minimize the ability of hackers to compromise the computing environment.

Even with thorough scanning and patching of affected software and systems, organizations will still be at high risk of a ransomware attack. Since the vulnerability was likely known to hackers for weeks before reaching public awareness in November last year, cybercriminals have had ample time to implant ransomware malware and backdoor viruses while the proverbial “front door” was unlocked. These tools can allow hackers access to vital systems, even if Log4J vulnerabilities are updated.

An additional item on security professional remediation checklists is backup software. One of the lesser-known targets of Log4j exploits include the agents of many popular backup and recovery products, which often provide access to a central data repository for all sensitive information in the organization.

Because of threats like Log4j, modern backup/recovery solutions should not rely on agents or the Java Naming and Directory Interface™ (JNDI) to avoid the exploits of Log4J and other threats such as ransomware, which in many cases are even more dangerous. Because many backup solutions are vulnerable, agent-based backup systems are now a necessity. If a backup environment is compromised, IT/backup administrators are advised to scan all existing data sets, quarantine suspected backups, scan live data sets for malware, and restart the backup of any compromised from known clean systems.

With the latest malware variants, data protection strategies and solutions utilizing air-gapped or immutable backups now provide a false sense of security and fall short in their defense against cyber threats. As a result, cyber-secure backup platforms are set to fill the voids inherent in these approaches. Asigra steps up to the challenge in three important ways:

1. Deep & Task-Specific MFA - Multi-factor authentication is the first step to prevent credential hunting attacks. MFA itself can be bypassed in some attacks, which is why Asigra embeds advanced user authentication deep into specific sensitive tasks.
2. Bi-directional Malware Scanning - Asigra uses an advanced malware engine capable of detecting 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. The system also scans files before they are restored.
3. Enterprise-class Data Security - Within the Asigra platform, data is protected at all times with the highest levels of security and compliance with AES 256-bit in-flight and at-rest data encryption, NIST FIPS 140-2 certification, Alternating Repository Naming to create a moving target for malware payloads, and Soft Deletes that provide a hidden/secret deletions folder that is accessible to the administrator.

“The art of data protection has evolved significantly over the past several years, making once standard features obsolete or even high-risk,” said Eric Simmons, CEO for Asigra. “This has exposed legacy platforms that require agents, leverage air gapping or rely on immutable backups. Asigra has advanced the state of data protection to provide a 100% agentless solution

and the most comprehensive suite of cyber defenses that make infiltration extremely difficult for even the most aggressive threat actors."

For a demonstration of this enhanced data protection suite, please contact info@asigra.com or visit https://www.asigra.com/contact-us to schedule.

Tweet This: @Asigra Cyber-Secure Backup Platform Defending Data Against Persistent Log4j Vulnerability - https://bit.ly/2N04LHu

Additional Resources:
- Download a comprehensive paper on this topic titled "Securing your backups against Log4J vulnerabilities" at https://info.asigra.com/lm-log-4j-whitepaper
- Hear what service providers have to say about working with Asigra: https://www.asigra.com/partnership.
- Follow Asigra on Twitter at: http://twitter.com/asigra
- View the enhanced features of the Asigra Hybrid Cloud Partner Program at: https://www.crn.com/slide-shows/cloud/300101651/2018-partner-program-guide-5-star-cloud-vendors-part-1.htm/pgno/0/7

About Asigra
Trusted since 1986, Asigra advanced AI-enabled data protection platform is proudly developed in and supported from North America, providing organizations around the world the ability to quickly recover their data from anywhere through a global network of IT service providers. As the industry's most secure backup and recovery solution for servers, virtual machines, endpoint devices, databases, applications, SaaS and IaaS based applications, Asigra protects sensitive data with anti-ransomware defense and 100% recovery assurance. The company has been recognized as a three-time Product of the Year Gold winner by Techtarget for Enterprise Backup and Recovery Software and positioned well in leading market research. More information on Asigra can be found at www.asigra.com.

###

Contact Asigra
Call 877-736-9901 or email info@asigra.com

Joe Austin
APR

+ 18183326166
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
