Bond Case Briefs

Municipal Finance Law Since 1971

Log4j Code Vulnerability Emboldens US Public Finance Cyber Attacks.

Fitch Ratings-New York/Austin-14 January 2022: The Log4j code vulnerability, nicknamed Log4Shell, could pose significant risk to public finance entities running Java-based software that incorporates the Log4j open source code, says Fitch Ratings. Public finance entities are broadly exposed due to the widespread use of Log4j, and bad actors will have ample opportunity to exploit the vulnerability. This could result in increased ransomware attacks, placing pressures on public finance entities' operations and finances. In addition, cyber insurance, which is increasingly cost prohibitive, may become unattainable for those entities that are not able to demonstrate robust cyber defenses.

Compromised systems can directly affect public finance entities in the near term through ransom payments and/or the costs of remediation and restoration of data and service. Over the longer-term economic disruption from cyberattacks could lead to loss of revenues for state and local governments and enterprises. The ratings impact of a cyberattack will depend on if an issuer has a material financial, operational, or reputational risk as a result of a breach, along with the effectiveness of disaster recovery and operational continuity plans. Pressures that result in a deterioration of financial metrics could lead to negative rating actions. Robust systems monitoring, capital investment in digital assets, regular software updates, network segmentation, and employee and management vigilance against phishing remain important safeguards against cybercrime.

Experts consider Log4Shell to be one of the most serious cyber security threats in decades, adding to an already challenging ransomware landscape. The US Cybersecurity and Infrastructure Security Agency (CISA) termed the vulnerability "critical" and documented international threat actors gearing up to exploit the vulnerability, advising vendors to prioritize software updates. However, due to the widespread use of the code, it will be difficult to identify and mitigate exposure quickly, and risks may not manifest for months if cyber criminals are able to plant malicious code before software is patched.

Log4j is an extremely common and highly configurable library of code that tracks changes and is used in any number of Java-based applications. A critical vulnerability was discovered on Dec. 9, 2021 that permits unauthorized access to Java-based applications and allows threat actors to insert malicious code into the Log4j framework. The vulnerability currently has no easy, comprehensive mitigation solution and allows hackers to adversely affect programs, data and computer networks.

Ransomware attacks on public finance entities have increased in the past three years. Log4Shell makes the risk of attacks more acute due to the ubiquity of Java-based software, the prevalence of a patchwork of legacy systems across the sector and the finite resources of IT staff. Many Java applications are unsupported or proprietary and organizations that do not have robust asset inventories of active applications may not be able to quickly identify embedded Log4j code. Additionally, the large costs of updating existing equipment and software generally mean that institutions, particularly smaller entities, may rely on legacy systems for many years, even with outdated or unsupported software, leading to gaps in institutional security.

Subsequently, proving a ‘clean bill of health’ with regard to Log4Shell may be difficult, further compounding the existing challenges that public finance issuers face in acquiring cyber insurance. Insurer guidelines necessitate ever more stringent security audits and adherence to industry best practices, such as staffing and system and software updates, in order to qualify for cyber insurance. Cyber insurance was already increasingly unaffordable for public entities with smaller budgets, with diminishing coverage limits and increasing insurance premiums, and Log4Shell will exacerbate this trend. For further discussion on cyber insurance costs, see our commentary Rising Insurance Costs Add to US Public Finance Cyber Pressures.

Contacts:

Omid Rahmani
Associate Director, US Public Finance
+1 512 215-3734
Fitch Ratings, Inc.
Terrace 1
2600 Via Fortuna, Suite 330
Austin, TX 78746

Sarah Repucci
Senior Director, Fitch Wire
Credit Research & Risk Analytics
+1 212 908-0726
Fitch Ratings, Inc.
Hearst Tower
300 W. 57th Street
New York, NY 10019

Media Relations: Sandro Scenga, New York, Tel: +1 212 908 0278, Email: sandro.scenga@thefitchgroup.com

The above article originally appeared as a post on the Fitch Wire credit market commentary page. The original article can be accessed at www.fitchratings.com. All opinions expressed are those of Fitch Ratings.