# CORPORATE VULNERABILITY STATEMENT: LOG4SHELL

TERAPAGE

www.terapage.ai

# Corporate Vulnerability Statement: Log4Shell

At Terapage, we are committed to maintaining the highest standards of cybersecurity and protecting the confidentiality, integrity, and availability of our systems and data. We recognize the recent identification of the Log4Shell vulnerability (CVE-2021-44228) as a significant security risk to our organization and the broader industry.

Log4Shell is a critical vulnerability discovered in the Apache Log4j logging library, which is widely used in many software applications, including our own. This vulnerability allows remote attackers to execute arbitrary code on affected systems, potentially leading to unauthorized access, data breaches, and disruption of our services.

We take this vulnerability very seriously and are actively monitoring the situation, staying updated with the latest information, patches, and recommendations from security experts and vendors. Our dedicated cybersecurity team is working diligently to assess the impact of Log4Shell on our systems, identify any potential exposures, and take immediate action to mitigate the risk.

In response to the Log4Shell vulnerability, we have implemented the following measures:

**1. Patch Management:** We have prioritized the deployment of vendor-recommended patches and security updates for the affected systems and applications. Our IT teams are working around the clock to ensure timely patching and minimize the window of vulnerability.

**2. Vulnerability Assessment and Penetration Testing:** We have initiated comprehensive vulnerability assessments and penetration testing exercises to identify any potential vulnerabilities introduced by the Log4Shell vulnerability. This helps us uncover any residual risks and validate the effectiveness of our mitigation measures.

**3. Monitoring and Incident Response:** We have enhanced our security monitoring capabilities to actively monitor for any suspicious activity or attempts to exploit the Log4Shell vulnerability. Our incident response protocols have been updated to include specific procedures to address and contain any potential incidents related to this vulnerability.

**4. Employee Awareness and Training:** We are conducting targeted awareness campaigns and providing updated training to our employees on the Log4Shell vulnerability, its potential impact, and

best practices to prevent and respond to security incidents. This ensures that our workforce remains vigilant and equipped to identify and report any suspicious activities promptly.

**5. Collaboration with Vendors and Industry Partners:** We are closely collaborating with our technology vendors and industry partners to stay informed about the latest developments, share insights, and leverage their expertise in addressing the Log4Shell vulnerability effectively.

As part of our commitment to transparency and accountability, we will continue to communicate openly with our stakeholders, including customers, partners, and regulatory bodies, providing updates on the actions taken, mitigations in place, and any additional steps necessary to address the Log4Shell vulnerability.

We encourage our stakeholders to remain vigilant, apply necessary updates and patches on their systems, and report any suspicious activities or potential security incidents promptly to our dedicated security team. Together, we can mitigate the risks associated with Log4Shell and ensure the security and resilience of our organization.

We remain committed to continuous improvement and investment in cybersecurity measures to safeguard our systems, protect our data, and maintain the trust of our stakeholders.

If you have any further questions or concerns regarding our response to the Log4Shell vulnerability, please reach out to our dedicated cybersecurity team at cyber@terapage.ai.

Terapage