新能安科技安全漏洞处理流程

一、基本原则

1. Ampace 高度重视产品与业务安全，承诺及时跟进、分析并回复所有漏洞报告。
2. 支持负责任的漏洞披露机制，对遵守白帽子精神的报告者给予感谢与奖励。欢迎企业、安全机构及研究者发现与提交安全漏洞。
3. 严禁利用漏洞实施数据窃取、系统入侵等违法行为，违者将追究法律责任。

二、漏洞处理流程

1. 漏洞报告

漏洞报告中格式不限，请写明漏洞复现过程。

2. 漏洞提交

发送报告至 zhanghc@ampacetech.com，我方收到后，会及时回复邮件。

3. 漏洞审核

1 个工作日内接收报告，7 个工作日内完成审核并邮件回复，必要时与报告者沟通。

4. 漏洞修复

Critical CVSS>=9	24 小时 - 7 天	24 小时内修复：适用于可导致业务瘫痪、数据大规模泄露或监管处罚的漏洞（如 Log4j2）。若需完整修复超过 24 小时，必须采取临时缓解措施（如关闭端口、防火墙拦截）。 云上服务≤48 小时热修复
High CVSS>=7	7 天 - 30 天	快速响应，制定修复计划并持续更新进展。
Medium CVSS>=5	30 天 - 90 天	纳入常规发布周期，风险可控下可结合版本迭代修复。
Low CVSS<5	90 天 - 180 天或者下一个版本周期	低风险漏洞可批量修复，结合系统升级或重构完成。

5. 流程闭环

验证修复完成后，流程终止。

6. 漏洞公告

已修复的漏洞，新能安科技将会在 SRC 页面或者公众号通告

三、漏洞定级标准

基于 CVSS 评分+业务影响综合评定，分 Critical/High/Medium/Low 四级。

四、补充说明

1. 禁止云端存储漏洞报告
2. 禁止借测试之名实施侵害行为
3. 仅受理 Ampace 产品及关联第三方业务漏洞
4. 同源漏洞取最高危级奖励
5. 同类操作漏洞合并处理
6. 复现未修复漏洞视为新漏洞
7. 仅奖励首位报告者
8. 严禁公开披露漏洞
9. 须提供有效 POC/截图/视频验证
10. CVE 漏洞披露后 3 个月内提交：首位有效报告者按中危上限奖励
11. CVE 披露 3 个月后提交：按常规流程处理，已跟踪漏洞视为已知

五、奖励机制

新能安科技对漏洞提交者由衷表示感谢，并颁发感谢证书。

六、争议处理

对流程/评级有异议者，可通过 zhanghc@ampacetech.com 申诉，AmpaceTech 将优先保障提交者权益。

Ampace Technology Security Vulnerability Handling Process

I. Basic Principles

12. Ampace places high importance on product and business security, committing to promptly follow up, analyze, and respond to all vulnerability reports.
13. We support responsible vulnerability disclosure mechanisms and express gratitude and rewards to reporters who adhere to white-hat ethics. We welcome enterprises, security organizations, and researchers to identify and submit security vulnerabilities.
14. It is strictly prohibited to exploit vulnerabilities for illegal activities such as data theft or system intrusion. Violators will face legal consequences.

II. Vulnerability Handling Process

1. **Vulnerability Reporting**
   No specific format is required for vulnerability reports, but please clearly describe the vulnerability reproduction process.
2. **Vulnerability Submission**
   Send reports to zhanghc@ampacetech.com. We will respond promptly via email upon receipt.
3. **Vulnerability Review**
   Reports are received within 1 working day, reviewed within 7 working days, and responded to via email. Communication with the reporter may be initiated if necessary.
4. **Vulnerability Remediation**

Critical CVSS>=9	24h – 7d	Fix within 24 hours: Applies to vulnerabilities that could cause business disruption, large-scale data leaks, or regulatory penalties (e.g., Log4j2). If full remediation exceeds 24 hours, temporary mitigation measures (e.g., port closure, firewall blocking) must be implemented. Cloud services: ≤48 hours for hotfix.
High CVSS>=7	7d – 30d	Quick response, formulate a remediation plan, and provide continuous progress updates.
Medium CVSS>=5	30d – 90d	Incorporated into regular release cycles; can be fixed during version iterations if risk is manageable.
Low CVSS<5	90d – 180d or next version	Low-risk vulnerabilities can be batch-fixed, combined with system upgrades or refactoring.

5. **Process Closure**
   The process is terminated after verifying the remediation is complete.
6. **Vulnerability Announcement**
   Fixed vulnerabilities will be announced on Ampace’s SRC page or official public account.

III. Vulnerability Grading Criteria

Vulnerabilities are graded based on CVSS scores combined with business impact, categorized into four levels: Critical, High, Medium, and Low.

IV. Additional Notes

1. Storing vulnerability reports in the cloud is prohibited.
2. Exploiting vulnerabilities under the guise of testing is prohibited.
3. Only vulnerabilities related to Ampace products or associated third-party services are accepted.
4. For vulnerabilities from the same source, the highest severity level reward is applied.
5. Similar operational vulnerabilities are processed together.
6. Unfixed vulnerabilities that are reproduced are treated as new vulnerabilities.
7. Only the first reporter is rewarded.
8. Public disclosure of vulnerabilities is strictly prohibited.
9. Valid Proof of Concept (PoC), screenshots, or videos are required for verification.
10. For CVE vulnerabilities submitted within 3 months of disclosure: The first valid reporter is rewarded based on the upper limit of Medium severity; internally tracked vulnerabilities may receive additional rewards.
11. For CVE vulnerabilities submitted after 3 months: Handled via standard procedures, and tracked vulnerabilities are considered known.

V. Reward Mechanism

Ampace sincerely thanks vulnerability reporters and issues certificates of appreciation.

VI. Dispute Resolution

For disputes regarding the process or grading, reporters can appeal via zhanghc@ampacetech.com. AmpaceTech will prioritize protecting the rights of submitters.