Kuaishou Security Vulnerability Management Rules

These rules aim to regulate the internal security vulnerability reporting format and the procedures of internal security vulnerability handling during different stages.

These rules are applicable to all data vulnerabilities of Kuaishou, including but not limited to the vulnerabilities found during internal scanning, external report, security analysis and penetration testing.

Sources of data vulnerabilities include, but are not limited to, the following channels: vulnerability scanning, security assessment, white box audit, external submission and internal testing.

Security vulnerabilities are classified into various categories, namely serious, high risk, medium risk, low risk and no impact/risk. For details of the vulnerability classification, please refer to the standards of the security emergency response center of Kuaishou at https://security.kuaishou.com/#/notice/detail?noticeId=2 (in Chinese)

These rules specify the procedures and rules for security vulnerability handling.