Threat	Vulnerability	Asset	Impact	Likelihood	Potential Risk Impact	Control Recommendations	Control Cost: monetary, Hours, Down Time
Information Leakage	Outdated OpenSSH (7.4-7.6)	Office Site B Router Office Site C Router Cloud DNS Office HQ VPN Office Site B VPN Office Site C VPN	High: Possibility of leaking sensitive user data	Moderate	Exfiltrate sensitive data Corporate Blackmail Potential $100,000 Loss	Update OpenSSH on all vulnerable machines	Monetary: None Can be handled in house Hours: 12 (Overestimation) Down Time: None
Kernel Memory Corruption	Outdated Ubuntu	Office Site C Router Office Site B Router Cloud Router Blipper Cloud Blipper App Cloud Blipper DB Florp Database Cloud Florp App	High: Possibility of privilege escalation	Moderate to High	Escalate privileges Exfiltrate sensitive data Corporate Blackmail Potential $100,000 Loss	Update the operating system on all vulnerable machines	Monetary: None Can be handled in house Hours: 20 Down Time: Significant (5 hrs per server)
Overflow XSS Bypass Code Execution Denial-of-Service	Apache 2.4.37	Cloud Monitoring	High: Possibility of privilege escalation, temporaray downtime	High	Escalate privileges Exfiltrate sensitive data Lose of potential monetary gains Corporate Blackmail Potential $100,000 Loss	Update to last version of Apache	Monetary: None Can be handled in house Hours: 3 (overestimate) Down Time: 3 hrs (overestimate)
Overflow Execution Code Overflow Bypass Directory Traversal Denial-of-Service	Ubuntu 16.04	Florp Database	High: Possibility of privilege escalation, temporaray downtime	High	Escalate privileges Exfiltrate sensitive data Lose of potential monetary gains Corporate Blackmail Potential $100,000 Loss	Update Ubuntu to latest version	Monetary: None Can be handled in house Hours: 3 (overestimate) Down Time: 3 hrs (overestimate)
SQL injection and arbitrary code execution	Outdated PostgreSQL	Cloud Code	High: Possiblility of privilege escalation	Moderate to High	Escalate privileges Exfiltrate sensitive data Corporate Blackmail Potenital $100,000 Loss	Update to lastest version PostgreSQL	Monetary: None Can be handled in house Hours: 3 (overestimate) Down Time: none
Double-Free Memory Corruption	Outdated OpenSSH	Cloud Monitoring Cloud Code Cloud Blipper App Cloud Blipper BD	Moderate: Could lead to a corrupt state of the memory manager	Moderate	Data Loss	Update OpenSSH on all vulnerable machines	Monetary: None Can be handled in house Hours: 12 (Overestimation) Down Time: None
Denial-of-Service	Alpine Linux 3.13	Blipper Cloud	Low: temporary downtime	Moderate	Lose of potential monetary gains Potential $1,000 - $10,000 Hourly Loss	Update Alpine to latest version	Monetary: None Can be handled in house Hours: 3 (overestimate) Down Time: none
Denial-of-Service	Outdated rpcbind	Cloud Router Blipper Cloud Monitoring Cloud DNS Cloud Code Cloud Mail Cloud Blipper DB Office HQ VPN Office Site B VPN Office Site C VPN	Low: Temporary downtime	Moderate	Lose of potential monetary gains Potential $1,000 - $10,000 Hourly Loss	Update the rcpbind on all vulnerable machines	Monetary: None Can be handled in house Hours: 12 (overestimate) Down Time: none