Security Incident Report Template

Incident identification

What happened?

|  |  |
| --- | --- |
| Action | Details |
| Incident reporter |  |
| Date and time of security incident |  |
| Time elapsed since the security incident was noticed by the [company] team |  |
| Details about the service(s) affected by the security incident |  |
| Details about whether customer data was exposed by the security incident |  |
| Severity of the security incident (Critical, High, Medium, Low) based on customer data exposure |  |

How did it happen?

|  |  |
| --- | --- |
| Action | Details |
| Details about the potential vulnerability that led to the security incident. (For example, a bad config/policy on AWS or a new package with a known vulnerability flagged by the CVE database) | Discovered an open S3 bucket with customer data |

|  |  |
| --- | --- |
| Detailed description of how the service(s) were affected by the security incident. (For example, an S3 customer data ingest bucket config/policy has read/write permissions by anyone on the internet. List all services using this S3 bucket and the potential impact on the customer’s data) |  |

What have we done since then?

|  |  |
| --- | --- |
| Action | Details |
| List detailed actions performed to fix the vulnerability detailed in the previous section |  |
| List other potential investigations done that might be vulnerable |  |
| Details about the fix/patch done to lock down further attacks |  |
| Tests reports clearly indicating that the deployed fix works |  |

Lessons Learned What are we doing to prevent this in the future?

|  |  |
| --- | --- |
| Action | Details |
| List the report from the investigations performed in the previous section |  |
| List all systemic improvements done to prevent future attacks |  |

Notification

What do you need to do?

|  |  |
| --- | --- |
| Action | Details |
| Notify the customer on specific steps needed to fix this problem. For example, enforce end users to download a security patch, download a new version of the app/sdk, etc. |  |
| List the customer support number for the end user to call should they have any questions |  |
| Has the incident resulted in a disclosure of confidential data?* *If no, end of incident analysis / evaluation*
* *If yes, notify appropriate parties*
 |  |