**REDBACK OPERTAIONS**

**VULNERABILITY FOUNDED-Encryption Key Exposure**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Is this a re-tested Finding?** |
| Pranav Sharma | Cybersecurity Team | Secure Code Review | No |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Risk Rating**  
Impact: Major  
Likelihood: Moderate

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

The exposure of the encryption key can lead to unauthorized access to encrypted data and compromise the confidentiality and integrity of the system.

**Location of vulnerability**

**sample\_receiver.py** and **sample\_sender.py** files.

**Evidence**

**A computer screen shot of a computer code

Description automatically generated**

**Remediation Advice**

Store encryption keys securely, such as in environment variables or encrypted configuration files.

Implement proper access controls to limit the exposure of sensitive information like encryption keys.

Rotate encryption keys periodically to mitigate the impact of key exposure.

**References**

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf\>

**Contact Details**

Pranav Sharma

222208296