

**Finding Name:** Exposed Encryption Keys

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Deakin Carr | SCR | SCR | Ontrack | Jaspriya kaur |  |

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

**Finding Description**

During the secure code review process, several instances of sensitive information being stored in plaintext were found. The findings include API keys and private keys within the .env.production file and the CAkeys directory. These keys are crucial for the security of the application, as they are used for encryption processes and authentication mechanisms.

**Risk Rating**  
Impact: Significant  
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 these sensitive keys poses a significant risk. Unauthorized access to these keys would allow attackers to decrypt sensitive data, execute privileged operations, and potentially gain full control over the application infrastructure. This could lead to data breaches, financial losses, and severe reputational damage.

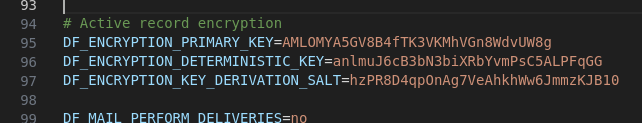
**Affected Assets**

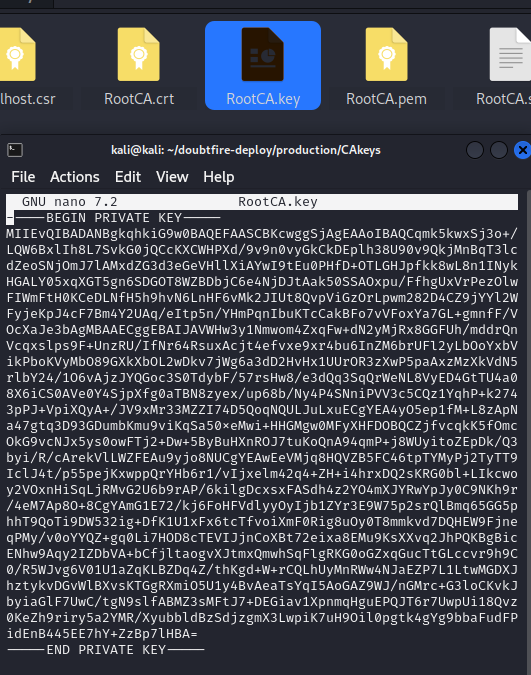
* .env.production file containing encryption keys
* RootCA.key and localhost.key files containing private keys

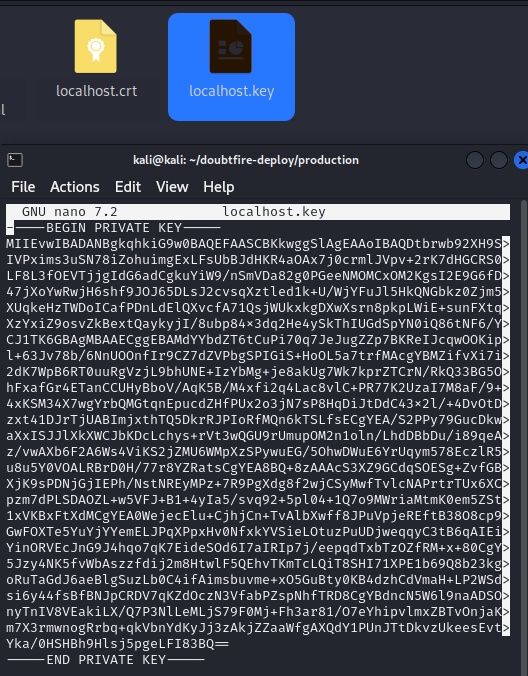
**Evidence**

To reproduce the vulnerability, follow these steps:

1. Clone the repository and navigate to the production directory.
2. Open the .env.production and localhost.key files in ~/doubtfire-deploy/production. Observe the plaintext secrets resembling the following pattern in .env.production:
   * DF\_ENCRYPTION\_PRIMARY\_KEY=AMLOMYA5GV8B4fTK3VKMhVGn8WdvU...
   * DF\_ENCRYPTION\_DETERMINISTIC\_KEY=anlmuJ6cB3bN3biXRbYvmPsC5ALPF...
   * DF\_ENCRYPTION\_KEY\_DERIVATION\_SALT=hzPR8D4qpOnAg7VeAhkhWw6Jmmz...
3. Access the CAkeys directory, open the RootCA.key , and notice the private keys stored in plaintext at the beginning of these files.







**Remediation Advice**

* Immediately rotate all exposed keys and secrets to prevent unauthorized use.
* Implement a secure secret management solution to handle sensitive information securely.
* Encrypt sensitive data at rest and ensure secure transmission channels are used to prevent unauthorized access.
* Regularly scan the codebase and environment files for exposed sensitive information and rectify the issues promptly.

**References**

GitLeaks. (n.d.). GitLeaks - A SAST tool for detecting hardcoded secrets like passwords, api keys, and tokens in git repos. Retrieved [3/4/24], from <https://gitleaks.io/index.html>

D. Gitlan, “Best Practices to Store the Private Key,” *SSL Dragon*, Last updated on February 20th, 2024, Available:https://www.ssldragon.com/blog/best-practices-to-store-the-private-key/

ChatGPT, “ChatGPT”, OpenAI [Large language model] Available: [https://chat.openai.com](https://chat.openai.com/) [Accessed: 2/4/2024].

**Contact Details**

DEAKIN CARR

Carrde@deakin.edu.au

**Pentest Leader Feedback.**

Great work Deakin. Can you add a screenshot as an example with the path so that your finding could be justified.  
  
Add screenshots to your work and use credible sources to justify your work –Roocha

- Hi Roocha, screenshots have been added. Added a reference as to why it is bad practice to store asymmetric private keys in plain text. I imagine you have determined that the ChatGPT reference is not a “credible source” - I am only referencing it as I used it to structure this document and per university policy I am required to cite it.