**We use CVE-2014-3508 as the instance for illustrating the work flow of VULTURE on patch commit mapping.**

1. **LLM-based description parsing**

## CVE-2014-3508 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Description

The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

As shown in CVE Description, two vulnerable elements are claimed: affected function "OBJ_obj2txt" and affected file "obj_dat.c".

2. **Slice-based commit locating**

   According to the affected versions claimed, it can be determined that the last vulnrable versioin is "1.0.1h" and the fixed version is "1.0.1i". By referencing the timestamp window related to the two versions and collecting commits wiithin this window, 106 commits are obtained.

   By dividing these 106 commits, a total of 6 slices were created (each slice containing 20 commits, with the last slice having 6 commits). We calculated the code differences between the first and last commits in each slice and compared whether these differences included vulnerable elements (the function "OBJ_obj2txt" and the file "obj_dat.c"). It was determined that only the 5th and 6th slices contained the relevant modifications, thus they were marked as candidate slices.

3. **Candidate commit selection**

   All commits within the two candidate slices were examined to determine whether their code changes included vulnerable elements (the function "OBJ_obj2txt" and the file "obj_dat.c"). If such elements were present, the commit was marked as a candidate.

   This step identified two candidate commits, with the hash values “03b04ddac162c7b7fa3c57eadccc5a583a00d291” and “abbd58559e9dfad09935d25105e2308f98f686d1.”

4. **LLM-based patch commit mapping**

   The LLM was invoked, with the CVE and its description, along with the commit messages and commit diffs of the two candidate commits, provided as input. Through prompting, the model was guided to determine which candidate commit was the target patch commit. The patch commit was successfully identified, with the hash value “03b04ddac162c7b7fa3c57eadccc5a583a00d291.”

   Upon verification, the commit message of the identified patch is as follows, and the result was confirmed to be correct.

   **Fix OID handling:**

   ```
   - Upon parsing, reject OIDs with invalid base-128 encoding.
   - Always NUL-terminate the destination buffer in OBJ_obj2txt printing function.

   CVE-2014-3508

   Reviewed-by: Dr. Stephen Henson <steve@openssl.org>
   Reviewed-by: Kurt Roeckx <kurt@openssl.org>
   Reviewed-by: Tim Hudson <tjh@openssl.org>
   ```