Vulnerability Assessment Report Template

Ime i prezime: Stasja Durutovic
Tim: 1
Datum: 03.11.2024.
Scan Tool: Nessus 10.8.3 (#10) WINDOWS
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID: CVE-2014-3707**

- **Opis: Ubuntu 14.04 LTS : curl vulnerability (USN-2399-1)**

Ova ranjivost je pronađena u programu curl i otkrivena je u verziji Ubuntu 14.04. Problem nastaje zbog nepravilnog rukovanja memorijom, što može dovesti do toga da osetljivi podaci budu pogrešno poslati na udaljeni server.

Port: 80 (HTTP) ili 443(HTTPS)

Protokol: HTTP/HTTPS, FTP, i drugi protokoli koji se koriste za prenos podataka.

Ova ranjivost može uticati na aplikacije koje koriste curl za slanje podataka na servere, omogućavajući napadaču da dobije pristup osetljivim informacijama koje se šalju. Na primer, ako se koristi za prenos lozinki, podaci mogu biti otkriveni, što predstavlja ozbiljan bezbednosni rizik.

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.8 (Critical)**
- **Vektor: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

Attack Vector : Network – eskploatacija može biti na određeni sistem ili mrežu (mrežni uređaji, mrežni protokoli, web serveri ili fizičke mrežne veze)
AC –Attack Complexity: Low – eksploatacija je jednostavna i ne zahteva kompeksne tehnike

PR- Privileges Required: None – nisu potrebne privilegije ili specijalne dozvole da bi napadač iskoristio ranjivost

UI –User Interaction: None - nije potrebna nikakva akcija korisnika

S- Scope: Unchanged – ne utiče na druge sisteme
C – **Confidentiality**: **None** – napadač ne može da pristupi poverljivim informacija

I- Integrity: High – eksploatacija može narušiti integritet podataka; napadač može da izmeni važne informacije

A-Availability: High – ima uticija na dostupnost, tako da može da uzrokuje pad sistema. Kada se usluga oslanja na curl za slanje ili primanje podataka, svaka eksploatacija ranjivosti može značiti da podaci neće biti dostupni ili da će se poslati pogrešno.

- **Opravdanje:**
  Ranjivost ima visok CVSS skor jer curl ima široku primenu u različitim aplikacijama i okruženjima. Napadači mogu iskoristiti ovu ranjivost bez potrebe za visokim nivoom tehničkog znanja, što znači da je eksploatacija potencijalno dostupna velikom broju napadača. Osim toga, uticaj na integritet doprinosu visokom skoru jer napadači mogu modifikovati ili slati osetljive informacije ka udaljenom serveru. Takođe, problem se može proširiti na veliki broj korisnika koji koriste određenu verziju curl-a.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne): Ne**
  Pretragom na Exploit-DB i GitHub-u nisam pronašla specifični eksploit koda koji se može koristiti za ovu ranjivost.
- **Opis eksploita: /**

- **Kod eksploita (ukoliko postoji):** /

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Ranjivost se odnosi na probleme u biblioteci libcurl 7.17.1, gde se tokom korišćenja funkcije CURLOPT_COPYPOSTFIELDS i curl_easy_duphandle() – funkcija libcurl bibliotke javlja greška u rukovanju memorijom koja može dovesti do otkrivanja osetljivih podataka. Ova greška postoji od kada je CURLOPT_COPIPOSTFIELDS uveden. CURLOPT_POSTFIELDS je opcija u cURL-u koja omogućava slanje podataka u HTTP

POST zahtevu. Funkcija curl_easy_duphandle() je pogrešno tretirala post podatke kao C string, što podrazumeva da se očekuje da string završi nul karakterom ('\0'). Međutim, podaci koji se šalju u POST zahtev mogu sadržati nulti byte ili ga čak nemaju, što može dovesti do različitih problema (prekomerno ili nedovoljno alociranje memorije, pad aplikacije, potencijalno curenje osetljivih informacija). Libcurl pošalje osetljive podatke u HTTP POST zahtevu, ukoliko se koristi specifičan niz funkcija — prvo CURLOPT_COPYPOSTFIELDS, a zatim curl_easy_duphandle().

Pogođene verzije: od libcurl 7.17.1 do i uključujući 7.38.0

Verzije na koje to ne utiče: libcurl < 7.17.1 i nakon i uključujući 7.39.0. Verzijom libcurl 7.39.0 se problem rešava.

Tačan commit: https://github.com/curl/curl/commit/a005243908803662d4a0542

- **Primer Koda (ako je primenljivo):** Nema dostupan specifičan primer koda koji direktno ilustruje ovu ranljivost, ali efekat se može videti kada se koriste opcije CURLOPT_COPYPOSTFIELDS i curl_easy_duphandle() u pogrešnom redosledu.

  ChatGPT :

```c
CURL *curl = curl_easy_init();
curl_easy_setopt(curl, CURLOPT_URL, "https://example.com");
curl_easy_setopt(curl, CURLOPT_COPYPOSTFIELDS, data);
CURL *duplicate_curl = curl_easy_duphandle(curl);
curl_easy_perform(duplicate_curl);
```

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):** Da. Patch za ranljivost CVE-2014-3707 je dostupan u verziji libcurl 7.39.0 i novijim verzijama.

- **MitigationStrategy:**
  Preporučuje se:

1. **Ažuriranje biblioteke**: Preporučuje se da korisnici odmah ažuriraju libcurl na verziju 7.39.0 ili noviju kako bi uklonili ranjivost. Ako trenutno nije moguća nadogradnja curl na novu verziju, treba preuzeti i primeniti dostupni patch koji rešava ovu ranjivost. Nakon primene, neophodno je ponovo kompajlirati libcurl kako bi izmene bile aktivne.
2. **Automatska rešenja**: Postoje alati i menadžeri paketa koji mogu automatski da primene ažuriranja (**APT (Advanced Package Tool)** za distribucije zasnovane na Debianu, kao što su Ubuntu: sudo apt update sudo apt install libcurl4; **YUM (Yellowdog Updater, Modified)** za distribucije zasnovane na Red Hat-u: sudo yum update libcurl; **Homebrew** za macOS: brew update brew upgrade curl
3. **Izbegavanje korišćenja CURLOPT_COPYPOSTFIELDS zajedno sa curl_easy_duphandle():** Kao alternativno rešenje, može se promeniti način na koji se koristi libcurl u kodu tako što se izbegava upotreba ovih funkcija u kombinaciji. Ovo neće rešiti problem unutar libcurl biblioteke, ali može sprečiti pojavu ranjivosti u kodu.
   Npr:

Synopsis

```
#include <curl/curl.h>

CURLcode curl_easy_setopt(CURL *handle, CURLOPT_POSTFIELDSIZE_LARGE,
curl_off_t size);
```

Description

```
curl_easy_setopt options                          CURLOPT_POSTFIELDSIZE_LARGE(3)



NAME
       CURLOPT_POSTFIELDSIZE_LARGE - size of POST data pointed to

SYNOPSIS
       #include <curl/curl.h>

       CURLcode curl_easy_setopt(CURL *handle, CURLOPT_POSTFIELDSIZE_LARGE,
                                 curl_off_t size);

DESCRIPTION
       If  you  want  to  post  data to the server without having libcurl do a
       strlen() to measure the data size, this option must be used. When  this
       option  is  used  you  can  post  fully binary data, which otherwise is
```

```
PROTOCOLS
       HTTP(S)

EXAMPLE
       CURL *curl = curl_easy_init();
       if(curl) {
         const char *data = large_chunk;
         curl_off_t length_of_data; /* set somehow */

         curl_easy_setopt(curl, CURLOPT_URL, "https://example.com");

         /* size of the POST data */
         curl_easy_setopt(curl, CURLOPT_POSTFIELDSIZE_LARGE, length_of_data);

         curl_easy_setopt(curl, CURLOPT_POSTFIELDS, data);

         curl_easy_perform(curl);
       }
```

Umesto korišćenja CURLOPT_COPYPOSTFIELDS, koristi se CURLOPT_POSTFIELDS zajedno sa CURLOPT_POSTFIELDSIZE_LARGE za slanje binarnih podataka. Ova metoda omogućava postavljanje veličine podataka bez potrebe za korišćenjem strlen(), čime se izbegavaju problemi koji se mogu pojaviti prilikom korišćenja niza koji može sadržati binarne podatke ili kada se podaci ne završavaju sa nulom.

Preporučeni alati: Dependabot ili Renovate: ovi alati mogu automatski da prate i biblioteke poput libcurl i OVS Scanner koji može da skenira projekte i identifikuje ranjivosti

- **Alternativni fix (ukoliko ne postoji vendorski): /**