Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenata: Vasilije Zeković i Milica Đumić  
Datum: 17.11.2024.

Pregled Ranljivosti

1.1 **Informacije o ranljivosti**ID ranljivosti (CVE): CVE-2014-3704  
Pogođen servis: Drupal  
CVSS ocena: 7.5  
Opis ranljivosti:

Slanjem *HTTP* *POST* zahteva, upotrebom *HTTP* protokola, korišćenjem porta 80 i *TCP* transportnog protokola, preko login stranice na *URI* *localhost/drupal/?q=node&destination=node,* sa parametrima koji su maliciozno definisani od strane korisnika, uspešno se izvršava *SQL injection* napad. Ovaj napad može dovesti do različitih zloupotreba nad bazom podataka, izvršavanjem proizvoljnih *PHP* skripti kao i instalacije *backdoors* programa. Direktno je pogođena metoda *protected function expandArguments(&$query, &$args)* apstrakne klase *abstract class DatabaseConnection extends PDO.* Pomenuta klasa i metoda pripadaju *Database Abstraction* sloju, koji omogućava podršku različitim bazama podataka.

1.2 **Opis eksploita**Izvor eksploita:

<https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/multi/http/drupal_drupageddon.rb>

Metod eksploatacije:

Potrebno je podesiti *URL* adresu sajta koju napadač cilja. Slanjem *HTTP POST* zahteva sa malicioznim parametrima na *login* stranicu se dodaje novi nalog u tabelu korisnika, a zatim se u tabeli uloga tom novododatom nalogu dodeljuje uloga administratora*.* U slučaju uspešne eksploatacije ranjivosti, napadač ima pristup novom administratorskom nalogu.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**Ranljiv cilj:  
(Opis podešavanja ranjive mašine - koja je verzija servisa, na kom port-u trči)  
Alati za eksploataciju:  
(Metasploit ili neki drugi alat, Python skripta, Perl skripta…)

2.2 **Koraci eksploatacije**Objasnite proces eksploatacije korak po korak - DETALJNO:  
(Uključite screenshot-ove celog procesa)

2.3 **Rezultat eksploatacije**Prikažite rezultate eksploatacije:  
(Uključite screenshot ekrana uspešne eksploatacije, dajte dokaz da ste eksploatisali sistem)

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 **Wazuh SIEM eravila**Pravila korišćena za detekciju:  
(Navedite specifična Wazuh pravila koja su se aktivirala ili prilagodila za detekciju eksploita)  
ID pravila:  
(Uključite ID pravila i kratak opis)

3.2 **Konfiguracija SIEM-a**Podešavanje Wazuh agenta:  
(Opis konfiguracije agenta na ranjivoj mašini i kako je povezan sa Wazuh Managerom)  
Prikupljanje logova:  
(Navedite koje logove pratite da biste otkrili pokušaje eksploatacije)

3.3 **Proces detekcije**Opišite proces detekcije:  
(Uključite logove ili screenshot-ove koji prikazuju da je napad detektovan pomoću Wazuha)

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**Opis integracije:  
(Objasnite kako je Wazuh integrisan sa The Hive-om za automatizovano kreiranje slučajeva)  
Integracija pravila:  
(Uključite kratak opis pravila koje pokreće kreiranje slučajeva u The Hive-u)

4.2 **Kreiranje slučaja u The Hive-u**Detalji o slučaju:  
(Dajte screenshot-ove koji prikazuju kreirani slučaj u The Hive-u nakon što se Wazuh pravilo aktiviralo)