UNIVERSITAS GADJAH MADA

Sample Penetration Test Report
Example Company

Company: Customer Name

UNIVERSITAS GADJAH MADA

Date: 07 July 2024
Version 1.0

Pendahuluan

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.

Ruang Lingkup

Evaluasi keamanan sistem informasi pada Cacti dilakukan di lingkungan produksi dengan melakukan upaya peretasan berdasarkan kerentanan yang ditemukan dan alamat IP yang diuji adalah sebagai berikut:

202.169.33.81
202.169.33.63
182.253.23.12
182.253.224.58
103.150.191.137

Metodologi

Metodologi yang digunakan dalam pengujian penetrasi ini terdiri dari beberapa tahap yang sistematis untuk memastikan pengujian yang menyeluruh dan efektif. Tahap-tahap ini meliputi information gathering, vulnerability scanning, vulnerability analysis, vulnerability exploitation, recommendation and reporting. Metodologi ini dirancang untuk mengidentifikasi dan mengatasi potensi celah keamanan dalam sistem secara menyeluruh.

Vulnerable Devices:

- 202.169.33.81: No CVE-2022-46169 Vulnerability Detected

- 202.169.33.63: No CVE-2022-46169 Vulnerability Detected

- 182.253.23.12: No CVE-2022-46169 Vulnerability Detected

- 182.253.224.58: No CVE-2022-46169 Vulnerability Detected

- 103.150.191.137: No CVE-2022-46169 Vulnerability Detected

Identifikasi Kerentanan

Pemindaian atau pencarian menggunakan Shodan dengan kata kunci "Cacti" memungkinkan untuk menemukan sistem-sistem yang menggunakan aplikasi Cacti.

202.169.33.81	80	Biznet Networks	2024-07-07T12:52:00.215457
202.169.33.63	80	Biznet Networks	2024-07-07T11:08:28.900158
182.253.23.12	80	Biznet Networks	2024-07-05T21:57:13.989305
182.253.224.58	80	Biznet Networks	2024-07-04T02:19:28.700079
103.150.191.137	80	PT Biznet Gio Nusantara	2024-06-29T19:46:16.618308

Shodan adalah mesin pencari untuk perangkat yang terhubung ke internet yang memberikan informasi tentang perangkat keras, perangkat lunak, konfigurasi, dan jenis layanan yang berjalan pada perangkat tersebut. Dengan menggunakan kata kunci "Cacti", Shodan akan mengembalikan hasil yang mencakup alamat IP dari sistem yang terdeteksi menggunakan aplikasi Cacti, port tempat aplikasi Cacti berjalan (umumnya pada port 80 untuk HTTP), nama penyedia jaringan atau organisasi yang terkait dengan alamat IP tersebut, serta tanggal dan waktu kapan data terakhir kali diambil atau sistem dipindai oleh Shodan. Contoh informasi ini menunjukkan bahwa beberapa alamat IP yang terhubung ke jaringan Biznet Networks dan PT Biznet Gio Nusantara menggunakan aplikasi Cacti pada port 80. Informasi ini memberikan pemahaman tentang di mana aplikasi Cacti diimplementasikan dan konteks infrastruktur jaringan yang digunakan.

Vulnerability Scanning

Vulnerability scanning dilakukan menggunakan perangkat lunak Metasploit. Metasploit adalah open-source, platform pengujian penetrasi berbasis Ruby yang memungkinkan pengguna untuk menulis, menguji, dan mengeksekusi kode eksploit. Sistem pengujian penetrasi atau pengujian pena bekerja dengan mensimulasikan serangan cyber untuk memeriksa kerentanan yang rentan. Dibawah ini menampilkan hasil dari pemindaian kerentanan yang ditemukan oleh Metasploit.

========== Vulnerability Scan Result for 202.169.33.81

This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[*] Using configured payload linux/x86/meterpreter/reverse_tcp

RHOSTS => 202.169.33.81
RPORT => 80
[*] 202.169.33.81:80 - The service is running, but could not be validated. Could not determine the Cacti version: the HTTP response body did not match the expected format.

========== Vulnerability Scan Result for 202.169.33.63

This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
RHOSTS => 202.169.33.63
RPORT => 80
[*] 202.169.33.63:80 - The service is running, but could not be validated. Could not determine the Cacti version: the HTTP response body did not match the expected format.

========== Vulnerability Scan Result for 182.253.23.12

This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
RHOSTS => 182.253.23.12
RPORT => 80
[*] 182.253.23.12:80 - The target appears to be vulnerable. The target is Cacti version 1.2.15

========== Vulnerability Scan Result for 182.253.224.58

This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
RHOSTS => 182.253.224.58
RPORT => 80
[*] 182.253.224.58:80 - The target is not exploitable. Target is not a Cacti application.

========== Vulnerability Scan Result for 103.150.191.137

This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.

[*] Using configured payload linux/x86/meterpreter/reverse_tcp
RHOSTS => 103.150.191.137
RPORT => 80
[*] 103.150.191.137:80 - The target appears to be vulnerable. The target is Cacti version 1.2.10

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.