# LibSSH

A computer screen shot of a computer screen

AI-generated content may be incorrect.

ამოცანის პირობის თანახმად flag-ის ძებნა მოსახერხებელია CVE-ის მეშვეობით. CVE-Common Vulnerability and Exposure. Exploit არ არის ვირუსი ანდ რაიმე malware. ის არის მიდგომა, რომელიც სისტემაში არსებულ მოწყვლადობას იყენებს თავდასხმის განსახორციელებლად.

A screenshot of a computer

AI-generated content may be incorrect.

სატიზე გადასვლისთანავე გვაქვს ssh-ის ინფორმაციაზე. SSH არის დისტანციურად ჰოსტზე დაკავშირების მიდგომა, რომელიც აბსოლიტურად უსაბრთხოა. ჩემი ამჟამინდელი ინფორმაციით, SSH-ის ბოლო ვერსია არის 2.0. გარდა SSH-ისა, გვაქვს libssh-ის შესახებ ინფორმაცია. Libssh C-Library არის, რომელიც SSH-ის კონფიგურაცია/იმპლემენტაციას უზრუნველყობს. ამოცანის პირობის თანახმად, flag-ის ძებნა CVE-ის მეშვეობით შეგვიძლია. მოვიძიოთ LibSSH-ის ამ ვერსიაზე ინფორმაცია, მოწყვლადი ხომ არ არის?



მოცემულ საიტზე გადასვლით ვადგენთ, რომ 0.6 და უფრო ახალი ვერსიების libssh მოწყვლადია. გარდა ამისა, CVE-იც მოცემულია. მოვძებნოთ გით-ზე source code:

A screenshot of a computer

AI-generated content may be incorrect.

  
მოცემული სკრიპტი argv-ს მეშვეობით იღებს ჰოსტის მისამართს, პორტსა და ბრძანებას. თუმცა სკრიპტი იმუშავებს იმ შემთხვევაში, თუ ssh კავშირი გვექნება ჰოსტთან:



ახლა გვრჩება მხოლოდ დირექტორიებში ძრომიალი და ფლაგის ძებნა 😊





გარდა ამისა, მაქვს დაწერილი სკრიპტი, რომელიც 2-1-ში მუშაობს და არ გვჭირდება ცალკე ssh-ის გაწერა და ცალკე სკრიპტის გაშვება.  
<https://github.com/giolga/ssh-command-exec>  
მოცემული სკრიპტი:

>ქმნის socket-ს და უერთდება მითითებული IP:Port მისამართით

>იყენებს paramiko ბიბლიოთეკას SSH პროტოკოლის გასამართად

>უვლის აუტორიზაციის პროცესებს გვერდს. კერძდ კი, სერვერს ატყობინებს, რომ მომხმარებელი აწ უკვე ავტორიზებული არის

> იქმნება SSH სესია და შესაძლებელია კომანდების გაშვება

