ShadowFax

The aim of this Pentest is to assess the security of a client's endpoint: ShadowFax. This report contains technical terms, but has been written so a non-technical reader with basic computing knowledge would understand it. The technical context will be provided in the Supporting Evidence section. Should the reader encounter difficulties understanding any technical section of the report, reading the "Executive Summary" and the "Conclusions and Recommendations" sections should provide enough context to the overall status of the pen-tested target. For further help, contact the help department.

Some Definitions

Hacker: A term given by the public that the cyber security industry more accurately called an attacker or intruder.

Vulnerability: Typically a bug or a misconfiguration in a computer program, or computer that can be abused to gain access to a computer

Exploit: A program or strategy to exploit a vulnerability.

Privilege Escalation: A technique to escalate privileges on a computer, often to an admin user.

Metasploit/Meterpreter: A tool designed to execute various vulnerabilities automatically. Helpful for Penetration Testing

Black Box Test: A penetration test without having any information beforehand of existing knowledge of the target.

{% embed url="https://pentestreports.com/reports/BitesPenTesting/penetration-test-report.html" %} Example Pen-Test Report {% endembed %}

Executive Summary

The pentest team provided a black box penetration test of the ShadowFax system to assess the security of all its operating system, applications, and running services. This penetration test was a manual exploitation of application-based and OS-based vulnerabilities. The target of the assignment covered Shadowfax which had the application AnyDesk installed. The team identified an outdated application and service, was able to run commands on the target, and achieve root compromise. Due to the severity of the exploits, it is advised that updates to the AnyDesk application are performed and removal of the SUID bit from the pkexe service are conducted to remediate the exposed vulnerabilities. Resources for remediation can be found below in the vulnerabilities section.

Target Overview

Hostname

IP Addresses	Network
10.0.6.52	shadowfax.shire.org (different subnet)
10.0.5.250	fw-rivendell.shire.org

Vulnerabilities

Severity (9.8 Remote Code Execution) - AnyDesk CVE: 2020-13160

- AnyDesk has a format string vulnerability that can be exploited for remote code execution. This allows for an attacker to establish a remote connection to the target and gain local access.
- Mitigation

  The solution is to update anydesk from 5.5.2 to version 7.1.5. Outdated software is often very vulnerable to exploits.

{% embed url="https://www.exploit-db.com/exploits/49613" %} Exploit used {% endembed %}

{% embed url="https://anydesk.com/en" %} New AnyDesk Download {% endembed %}

Severity (7.9 High) - PwnKit CVE: [2021-4034]

- This vulnerability allows for local privledge escalation through polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands (NIST).
- Mitigation

  There are a few mitigations in order to resolve this vulnerability. The first is to remove the SUID bit from pkexec using *0755 /usr/bin/pkexec.* In addition, performing regular audits will help find vulnerabilities before the become a problem. The biggest solution is keeping software and OSs up to date.

{% embed url="https://nvd.nist.gov/vuln/detail/cve-2021-4034" %} NIST CVE Site Page {% endembed %}

{% embed url="https://sysdig.com/blog/detecting-mitigating-cve-2021-4034-sysdig/" %} Pwnkit Mitigation Source {% endembed %}

Supporting Evidence

Prerequisites

The pen-test of ShadowFax requires the previous exploitation of fw-rivendell (WordPress target). The target is hosted on the 10.0.6.0 subnet so fw-rivendell will be used as a pivot machine. For instructions on how fw-rivendell was exploited see the fw-rivendell report below.

{% embed url="https://technotes.noahbeckman.com/v/sec480-pentest-2/targets/borormir" %} fw-rivendell Pen-test Report {% endembed %}

Scanning and Enumeration

The first step to enumerating ShadowFax was to set up a proxy. The target machine is hosted on a different subnet so proxy chains sends network traffic through fw-rivendell. This allows for scanning tools and exploits to be run on my pentest machine versus downloading them to fw-rivendell.

The next step was to scan the target. This can be seen in a screenshot below.

Nmap scan of target

There are 3 key ports open on the target. SSH using 22, and Anydesk using 7070 and 50001. when trying to navigate to the 7070 webpage no connection can be made. However, we can pull the SSL certificate from the port.

SSL Certificate

Shadowfax SSL cert

The SSL cert gives confirmation that Shadowfax is using Anydesk on port 7070. After research on AnyDesk vulnerabilities, it is found that it uses port 7070 for TCP and 50001 for UDP. This will be important later.

Foothold

Vulnerability Research

Using Google and Searchsploit, I was able to find the following AnyDesk vulnerability. It uses a buffer overflow to exploit an RCE and create a reverse shell. In order to configure the exploit, some custom shellcode has to be created. This can be done using a program called MsVenom.

MsVenom Payload Creation

MSVenom Payload

The payload above creates a reverse TCP shell to my kali machine on port 5552. the shellcode is then copied and placed into the AnyDesk exploit.

AnyDesk RCE Vulnerability

Screenshot of custom edited payload

The exploit can be seen above. Now for the exploit to execute on the target, there is an issue. ProxyChains forwards commands over TCP. However, the exploit has to be sent to the 50001 port over UDP. In order to get this to work, a program called Socat needs to be setup. Socat is a bidirectional relay for packets. We can create a socat relay from kali to Elrond on fw-rivendell UDP:<customPort> to TCP:<Customport>. Then on fw-rivendell, make another relay going from fw-rivendell to ShadowFax TCP:<CustomPort> to UDP:<50001>. Further instructions can be found below.

Setting up Socat

{% embed url="https://technotes.noahbeckman.com/v/sec480-pentest-2/useful-things/socat" %} Setting up Socat {% endembed %}

Gaining a reverse shell

reverse shell

This screenshot shows the reverse shell of the exploit. We can see the Shadowfax user flag and other directories. While using Netcat to catch the reverse shell is great, we really want to use Metasploit so we can use its modules for privilege escalation.

Upgrading shell

In order to easily do the privilege escalation, the reverse shell should be a Meterpreter connection. For instructions on how to do this in Metasploit, refer to the guide below.

{% embed url="https://technotes.noahbeckman.com/v/sec480-pentest-2/useful-things/metasploit-shells" %} Creating and Upgrading shells in Metasploit {% endembed %}

Getting the reverse shell connection

user flag contents

Privilege Escalation

Privilege escalation typically starts out with searching through currently running services, SUID bits, and more. The program Linpeas.sh is typically another good start that automatically runs through most of the checks. Often times this gives us the best place to look not an actual vulnerability.

Enumeration

After running Linpeas, it returns that the PwnKit vulnerability is exploitable on Shadowfax. There is a Metasploit module for it also.

PwnKit CVE

The configuration for the PwnKit exploit consists of the target host, port, and active Meterpreter session.

running the exploit

root flag

The exploit returns a new Meterpreter session with root-level access. This can be seen in the screenshot above showing the root flag contents.

Persistence

Most malicious actors will establish some form of persistence in the environment they attack. For the sake of the pentest, a user with admin privileges was created. Unfortunately, due to other people attempting to exploit the box my persistence was removed since the target got reverted.

User creation and modding

SSHed into my account and in sudo group

Post Exploitation (Loot)

{% embed url="https://app.gitbook.com/s/ARbxojkXZUSOB608QVbo/tools-and-loot/loot" %} Loot Page {% endembed %}

Conclusions and Recommendations

In conclusion, ShadowFax has critical vulnerabilities that lead to total compromise. As described in the Vulnerabilities section, updating software and the operating system would remove these issues from the environment. Root compromise is a big issue as malicious actors can exfiltrate data, delete or manipulate confidential information, and much more. This needs to be addressed ASAP.

Lab Issues

This lab did not present a lot of issues. However, learning how to use socat and upgrade a Metasploit connection (again) was kind of difficult. I made sure to make supplemental documentation to reference in the future.