Art's Tailor Shoppe Penetration Test Report

Pr0b3.com

2021-12-16

Contents

Executive Summary

Background

Art's Tailor Shoppe purchased penetration testing services from Pr0b3.com. Pr0b3.com was given permission to test Art's Tailor Shoppe's network and computer systems (CIDR 217.70.184.0/24), wireless network, web application, and mobile application. The penetration test allows for social engineering and testing for vulnerabilities past the discovery of an initial vulnerability.

Goals

One goal of the assessment is to protect Art's Tailor Shoppe from being successfully attacked from the internet. Another goal is to minimize damage done to the business if the network should be breached. Overall, the main goal is to prevent confidential information from being stolen and keep the business running smoothly.

Overall Posture

The overall security posture of Art's Tailor Shoppe was determined to be quite bad. Multiple passwords used were easily brute-forced or found in publicly available password lists. There were multiple cases of passwords being stored or transmitted in plaintext. Default credentials were still in use for at least one service. Software with critical vulnerabilities had gone unpatched for years. Some of these vulnerable versions were exposed to the internet. However, some required authentication or network access. At least three application security vulnerabilities discovered were not the result of outdated software, but instead mistakes that developers had made when creating the custom software. Operational security needs improvement because some information discovered from eavesdropping and dumpster diving was actionable for attackers.

Risk Ranking/Profile

We believe Art's Tailor Shoppe to have a high risk of being attacked and breached by threat actors. Many vulnerabilities were trivial to find and could easily be identified from the internet with automatic scans. An attacker with only a slight motivation to cause harm to Art's Tailor Shoppe could probably do so. For each report, we have assigned a risk rating of LOW, MODERATE, HIGH, or CRITICAL. These ratings serve to indicate how the vulnerabilities should be prioritized when remediating, and what the potential impact of exploitation is.

Summary of Findings

Our findings consist mostly of weak and default credentials, the use of software with known vulnerabilities, and vulnerabilities in custom software. Some

vulnerabilities discovered were the result of operational security failures, or software misconfigurations.

Recommendation Summary

Many vulnerabilities can be remediated by updating software. Some vulnerabilities may require changing the configuration of software or even changing the software of applications. Employee passwords need to be strong and default credentials should be changed.

Strategic Roadmap

We recommend remediating each of our findings in order of highest severity to lowest severity. Then, we recommend training for employees to encourage secure development and password practices. Afterwards, keep an inventory of assets and the versions of software they use. Regularly patch known vulnerabilities every week, and undergo penetration testing every 6 months.

Technical Report

Finding: *Nameserver allows mapping of internal network*

Affected asset: 10.70.184.38

Risk Rating

We give this vulnerability a LOW risk rating. This vulnerability would allow an external attacker to map out the internal network by querying the nameserver. This has no direct security impact, but may allow an attacker to identify interesting machines to target if the network is breached later.

Vulnerability Description

When querying the nameserver for hostnames and ips, the nameserver will provide information for internal IP addresses from outside the network.

Confirmation method

To confirm the vulnerability still exists, run the command

```
dig @217.70.184.38 costumes.artstailor.com
```

from outside the internal network. If the nameserver responds with an internal IP address, the vulnerability still exists.

Mitigation or Resolution Strategy

To mitigate, the nameserver should check to see if the DNS query originates from within the internal network before responding with a private IP.

Finding: *Lack of HTTPS*

Affected asset: www.artstailor.com

Risk Rating

We rate this vulnerability as LOW because it requires an attacker to be positioned between the client and server in the route between the two, but may lead to sensitive data exposure.

Vulnerability Description

The web server at www.artstailor.com has HTTP but not HTTPS enabled, causing all web traffic to and from the server to be transmitted in cleartext. An attacker, in some circumstances, can view this traffic.

Confirmation method

To confirm that the vulnerability still exists, try visiting https://www.artstailor.com. If this fails, redirects, or displays an error, the vulnerability still exists.

Mitigation or Resolution Strategy

Use a TLS certificate, enable HTTPS (port 443) traffic, and redirect traffic intended for port 80 to port 443.

Finding: *VSFTPD Backdoor Command Execution*

Affected asset: www.artstailor.com

Risk Rating

We rate this vulnerability as CRITICAL because it allows for command execution on the host and can be easily identified by scanners.

Vulnerability Description

There is an outdated version of vsftpd (2.3.4) listening on port 21. This version is vulnerable to Backdoor Command Execution (CVE-2011-2523). There is an exploit publicly available here.

Confirmation method

To confirm that the vulnerability still exists, run nmap -sV www.artstailor.com and check for the version of vsftpd on port 21. If it is version 2.3.4, it is still vulnerable.

Mitigation or Resolution Strategy

To Mitigate, update vsfptd to the latest version.

Finding: *Buffer Overflow*

Affected asset: www.artstailor.com

Risk Rating

We assign a risk rating of HIGH to this vulnerability because it allows an external attacker to execute any commands as the user ”brian” on the www.artstailor.com server.

Vulnerability Description

There is a service listening on port 1337. After providing the username ”brian”, the service provides a list of allowed commands that can be run. However, this list can be overwritten through a buffer overflow, and any commands can be executed.

Confirmation method

To confirm that the vulnerability still exists, run

```
nc www.artstailor.com 1337
```

and provide the username ”brian” to the service. Then, when prompted for a command, send

```
11111111111111111111111111111ls
```

If ”ls” is one of the allowed commands in the response, the vulnerability still exists.

Mitigation or Resolution Strategy

To mitigate, validate the length of the string being copied to the buffer, or use a memory-safe programming language.

Finding: *Router Administration Panel Accessible From The Internet*

Affected asset: innerouter.artstailor.com

Risk Rating

We assign a risk rating of LOW to this vulnerability, because it does not directly lead to the compromise of systems or business operations. It opens up the possibility for exploitation but is not directly exploitable.

Vulnerability Description

There is a service listening on port 8443 of the innerouter host (217.70.184.3) that allows users to remotely change the router's configuration, including port forwards and firewall rules. This panel requires authentication to access, but should ideally be inaccessible from the internet.

Confirmation method

To confirm that the vulnerability still exists, navigate to https://217.70.184.3 from the external network. If the pfSense sign-in screen is shown, the vulnerability still exists.

Mitigation or Resolution Strategy

To mitigate, set strict firewall rules allowing access to the web management interface to only LAN IP addresses. For more information, see the pfSense guide.

Finding: *Default Router Credentials*

Affected asset: innerouter.artstailor.com

Risk Rating

We assign a risk rating of HIGH to this vulnerability, because it allows external hosts to connect to any services on any host in the network.

Vulnerability Description

The innerouter host (217.70.184.3) uses default credentials for its web management interface, which are publicly known. This allows threat actors to gain control of the router and change its configuration.

Confirmation method

To confirm that the vulnerability still exists, try to log in to the pfSense router's web management interface with the default credentials (admin:pfsense). If authentication succeeds, the vulnerability still exists.

Mitigation or Resolution Strategy

To mitigate, we recommand changing the credentials for the router, as is instructed in the web management interface upon logging in.

Finding: *Weak Active Directory Password Policy*

Affected assets: all Windows hosts

Risk Rating

We assign a risk rating of MODERATE to this vulnerability, because it may lead to the compromise of user accounts.

Vulnerability Description

The active directory password policy allows weak passwords for users, making the compromise of user accounts through password spraying more likely. For more information on password spraying, check the Attack Narrative section.

Confirmation method

To confirm that the vulnerability still exists, check the password policy by running

```
Get-ADDefaultDomainPasswordPolicy
```

Mitigation or Resolution Strategy

Change the password policy to require longer, more complex passwords. You should not require users to periodically change their passwords, as this may encourage users to use easily guessable/memorable passwords. Passwords should be required to be at least 8 characters long, and passwords must be allowed to be at least 64 characters long. The password policy should require special characters but also check the provided password against a list of commonly used passwords, and reject those passwords from being used. Even with password length and complexity requirements, users may choose to use easily guessable passwords. To prevent user accounts from being compromised, we recommend reminding employees to use difficult-to-guess passwords and requiring two factor authentication.

Finding: *Privilege Escalation through DLL Hijacking*

Affected asset: costumes.artstailor.com

Risk Rating

We rate the risk of this vulnerability as MODERATE because the vulnerability requires local user access to exploit.

Vulnerability Description

An attacker is able to escalate privileges from the s.wilkins user to an administrator account by writing a DLL in a folder that is searched by a privileged process or service. This folder is

```
C:\Users\s.wilkins\AppData\Local\Microsoft\WindowsApps
```

Confirmation method

To confirm that the vulnerability still exists, check to see if the s.wilkins user has write permissions for the WindowsApps folder (above).

Mitigation or Resolution Strategy

Remove write permissions for any users that are not administrators for the WindowsApps folder.

Finding: *Privilege Escalation through Service Abuse*

Affected asset: costumes.artstailor.com

Risk Rating

We rate the risk of this vulnerability as MODERATE because the vulnerability requires local user access to exploit.

Vulnerability Description

The s.wilkins user has permissions for the BITS service, allowing the configuration to be changed and ultimately, commands to be run as a privileged user.

Confirmation method

Check to see if the s.wilkins user has too many permissions for the BITS service by executing

```
sc sdshow BITS
```

For more information, see here

Mitigation or Resolution Strategy

Remove permissions for the s.wilkins user for the BITS service so that the configuration can not be changed.

Finding: *Use of LM Hashes*

Affected asset: costumes.artstailor.com

Risk Rating

We assign a risk rating of LOW to this vulnerability, because it requires privileged access to a system and NT hashes can still be cracked.

Vulnerability Description

User hashes are stored as LM hashes, which use a weak algorithm and can easily be cracked with modern computing power.

Confirmation method

Check the group policy security options for "Do not store LAN Manager hash value on next password change", and see if it is disabled. If it is disabled, the vulnerability still exists.

Mitigation or Resolution Strategy

Change the previously stated setting (from Confirmation Method) to be enabled, then change all user passwords.

Finding: *Insecure Transmission of Cleartext Password*

Affected asset: ceo.artstailor.com

Risk Rating

We assign this a risk rating of a MODERATE, because it requires an attacker to have access to the internal network, but allows plaintext credentials to be stolen.

Vulnerability Description

An attacker can spoof a WAPD response and cause requests meant for pdc.artstailor.com to be intercepted.

Confirmation method

To confirm that LMMNR is still in use, run

```
tcpdump -i ens32 udp port 5355
```

from a host inside the network and check for communication.

Mitigation or Resolution Strategy

We recommend configuring all web browsers (especially for ceo.artstailor.com) to only use DNS (disable autodetect proxy settings). We also recommend using HTTPS and TLS whenever possible.
Optionally, create a DNS entry for wpad.artstailor.com to prevent the use of LLMNR to locate that host.

Finding: *Sensitive File Disclosure*

Affected asset: www.artstailor.com

Risk Rating

We assign a risk rating of HIGH to this vulnerability, because it exposes a username and password hash.

Vulnerability Description

Through the
/brian/getimage.php?raw=true&file=htpasswd
route, a username and password hash can be disclosed to an unauthenticated attacker.

Confirmation method

To confirm that the vulnerability still exists, visit
http://www.artstailor.com/brian/getimage.php?raw=true&file=htpasswd
and see if the contents of the file are disclosed.

Mitigation or Resolution Strategy

Move the htpasswd file to a different folder and prevent the php file from accessing files outside of the intended folder.

Finding: *Unrestricted File Upload*

Affected asset: www.artstailor.com

Risk Rating

We assign a risk rating of HIGH to this vulnerability, because it allows an authenticated attacker to execute commands as the www-data user on the www.artstailor.com host.

Vulnerability Description

At the admin panel at /brian/imgfiles/upload.php route, an attacker can upload any file type to the /brian/imgfiles/ route. This allows command execution through the uploading of a PHP webshell.

Confirmation method

To confirm that the vulnerability still exists, send a PHP webshell with the file extension of ".png", but intercept the request with a web proxy and change the file type to ".php". Then, visit the webshell in /brian/imgfiles/{filename.php} to run your commands.

Mitigation or Resolution Strategy

Verify on the server-side application that the file extension matches ".png" or ".jpg". Remove any created webshells, including pr0b3sh3ll.php.

Finding: *Lack of Certificate Verification for Wireless Router*

Affected assets: devices connecting to the artstailor-ddwrt-1 router

Risk Rating

We assign a risk rating of MODERATE because it requires access to a machine in the proximity of the local network but allows password hashes to be collected.

Vulnerability Description

The client being used by brian to connect to the router does not provide a ca_cert, which is used to verify the identity of the server. This allows an attacker to impersonate the router and collect credentials intended for the router.

Confirmation method

Spoof the router's SSID with:

```
sudo airmon-ng check kill

sudo airmon-ng start wlan0
```

```
sudo airodump-ng wlan0mon
```

```
sudo airmon-ng stop wlan0mon
```

Change the hostapid configuration file to use the SSID ”artstailor-ddwrt-1”, then run

```
sudo ./hostapd-wpe hostapd.conf
```

If the challenge, response, or NETNTLM hash can be interecepted with this method, the vulnerability still exists.

Mitigation or Resolution Strategy

Verify the router's identity by providing a ca_cert and ca_path (if using wpa_supplicant to connect).

Finding: *Hardcoded Credentials*

Affected asset: mobile application

Risk Rating

We assign a risk rating of MODERATE to this vulnerability, because it allows other applications to have access to the database.

Vulnerability Description

The android application uses hardcoded credentials to connect to a local database, potentially exposing sensitive information to other applications on the device.

Confirmation method

Search through the application source code and find the credentials. If they are still there, the vulnerability probably still exists. To completely make sure, try to connect to the database with the credentials.

Mitigation or Resolution Strategy

Implement a more secure way of connecting to the database, if the database is found to be necessary. This can include generating a random but secure set of credentials for each device. If the database is unnecessary, do not connect to it at all.

Finding: *Backup Domain Controller Vulnerable to EternalBlue*

Affected asset: 10.70.184.89

Risk Rating

We assign a risk rating of CRITICAL to this finding, because it allows an attacker with network access to gain access to the Domain Administrator account, which essentially has control over every windows host on the network.

Vulnerability Description

The unfinished Backup Domain Controller host uses an outdated version of the Windows Server that is vulnerable to the EternalBlue exploit. This exploit abuses the SMB service of the host to gain NT AUTHORITY/SYSTEM access.

Confirmation method

To confirm that the host is vulnerable to EternalBlue, run the nmap script

```
nmap -sC -p445 -open -max-hostgroup 3
      -script smb-vuln-ms17-010.nse 10.70.184.89
```

from another host on the network (devbox maybe).

Mitigation or Resolution Strategy

Update the Windows Server to patch against EternalBlue.