Final Project Presentation

Cyber Security Final Project

Karen Taylor

Intro

Presenter:

Karen Taylor
Cyber Graduate
SCI powered by Woz-U Cyber Security Program

Agenda: Vulnerability Reports

1. Critical Severity
2. High Severity
3. Medium Severity
4. Low Severity

Vulnerability Overview

Critical: **CVE-2022-41924** Vulnerability Identified in the Tailscale Windows Client.

High: **CVE-2020-3133** Affecting Cisco Email Security Appliance

Medium: **CVE-2020-3345** Vulnerability in the SonicOS SSLVPN Software.

Low: **CVE-2020-3585** Affecting Cisco Firepower Series 1000 Firewall Software

Critical Severity Report

1

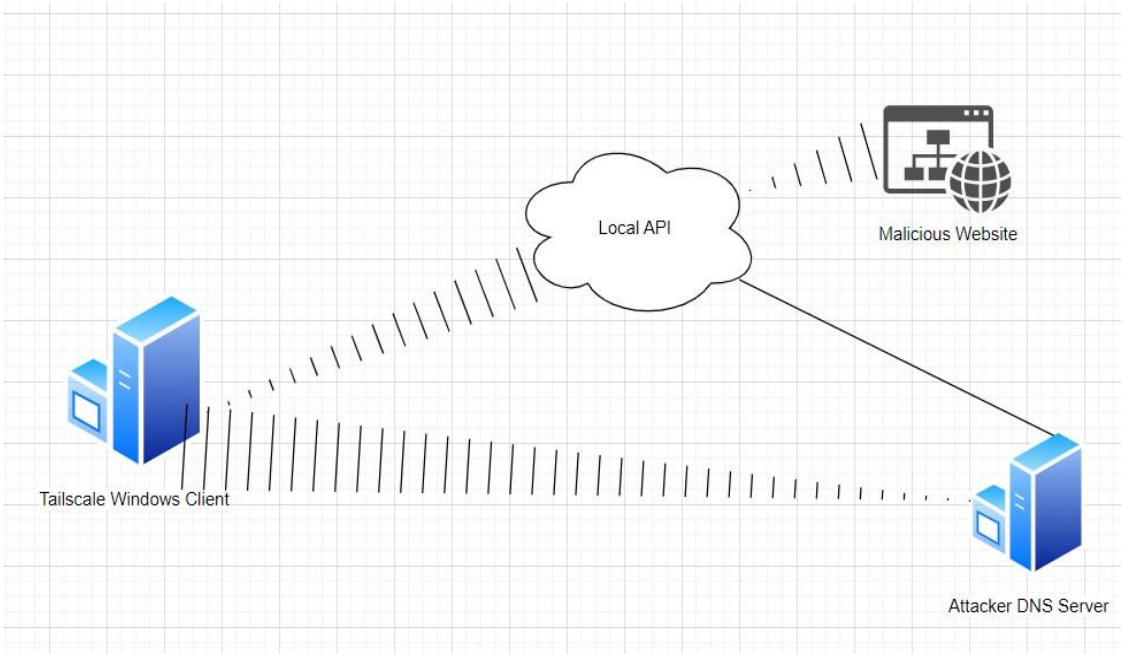
Vulnerable System and/or Service: Vulnerability identified in the VPN Tailscale Windows Client.

Vulnerability Description: A vulnerability identified in the Tailscale Windows client allows a malicious website to reconfigure the Tailscale daemon which can then be used to remotely execute code on the window client network. All Windows clients prior to version v.1.32.3 are affected. Tailscale VPN lets you easily manage and access your devices and resources quickly on your network, and you can work securely from anywhere in the world. And the true benefit of Tailscale is when building on top of a secure network system, Tailscale can offers speed, stability, and simplicity over traditional VPNs.

Summary of Attack:

The API allowed an unauthenticated attacker to send haphazard commands to the Windows client GUI, which were executed with the privileges of the logged in user. There was no Host header verification (The HTTP Host header is a request header that chooses the domain client (browser) wants to access.) If the Http Host header is not validated correctly, an attacker can supply invalid input to the servers. An attacker-controlled server can send malicious URL responses to the client computer, including pushing executables files on the network. This vulnerability could allow attackers to stage remote code execution (RCE) attacks, gain access to sensitive data, or launch denial of service (DoS) attacks.

2



Critical Severity Report

3

How to Prevent This Type of Attack:

1. Verify Host Header

2. Upgrade Tailscale clients in a timely manner

3. Disabling unnecessary ports.

4. Set permissions for who can connect to the network

5. Scan for vulnerabilities, and provide alerts when they are detected

4

How to Recover if Attacked:

1. Since Tailscale does not automatically update itself, users should make sure they are running v1.32.3 or later. So, update to the latest version of Tailscale.

2. You can also Uninstall Tailscale

3. Then Delete the user profile

4. After that Reinstall Tailscale

High Severity Report

1

Vulnerability Description: A Cisco Email Security Appliance could allow emails with malicious content to pass through the device. The vulnerability is due to improper validation of incoming emails.

Cisco Email Security Appliance is supposed to detect, block, and remediate incoming threats.

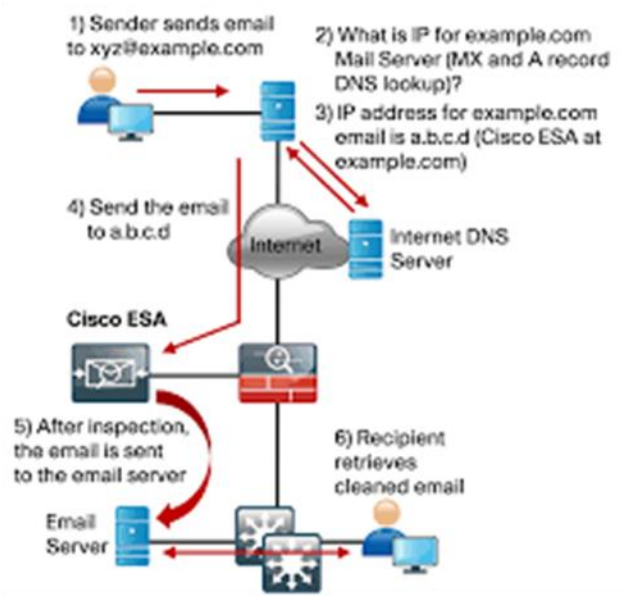
The attacker can exploit the appliance vulnerability and bypass its filters to get malicious content through the device.

Employee who believes that all email has been thoroughly filtered accidentally opens an email with malicious attachments.

The malicious code starts to embed itself into the network.

cisco Cisco Email Security

2



High Severity Report

3

How to Prevent this Type of Attack:

Download and Install the Cisco software update that addresses the vulnerability.

Conduct Routine Security Training for employees to keep them up to date in latest attacks.

Install an Email Security Gateway on the network.

Implement Multi Factor Authentication for all network systems.

Implement a Company Email Policy that defines what is acceptable use of business email.

4

How to Recover if Attacked:

A successful attack would allow an email with malicious code to get into the business email system.

Disconnect from the internet and disable remote access.

Maintain Firewall settings and install any pending security patches.

Isolate the threat and focus on the affected device or workstation.

Restore factory settings and reset passwords for the Cisco appliance.

Review all of the network logs to find any suspicious activity.

Ensure employees change passwords and also attend security training on a regular basis.

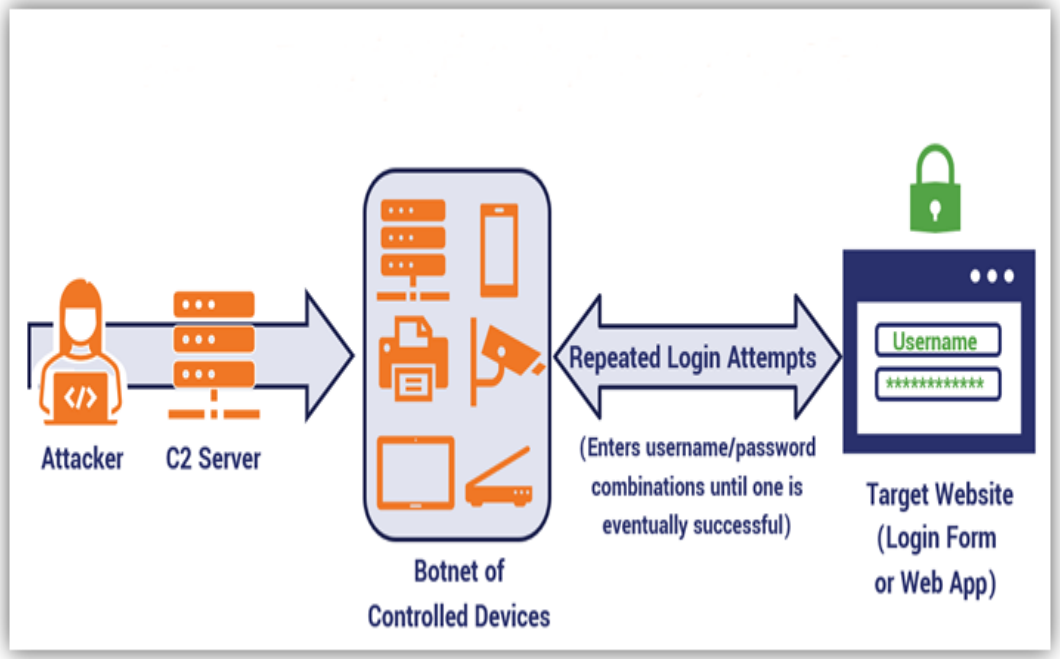
Medium Severity Report

1 **Vulnerable System and/or Service**: SonicOS SSLVPN network.

Vulnerability Description: Poor set-up of the SonicOS VPN network created a vulnerability which allowed the attacker access to the network.

Summary of Attack : A lack of best proper security implemented causing the VPN to be vulnerable. Thus, granting the attacker access to the network. Proper set-up of the SonicOS VPN Network should have stopped the multiple failed attempts, but it didn't, this makes the software vulnerable to brute force attacks. A brute force attack is a type of cyber attack in which an attacker uses automated software to rapidly and systematically attempt to guess the correct username, password, or personal, also the attacker uses trial-and-error methods to guess the correct credentials until they are successful.

2



Medium Severity Report

3

How to Prevent this Type of Attack:

1. Restrict the number of login attempts and enable administrator/user lockout in the of the software.
2. Use two-factor authentication
3. Use strong passwords: Using strong passwords that are difficult to guess is an effective way to prevent brute force attacks.
4. Implement CAPTCHA
(is a challenge-response system used to ensure that a human is interacting with the system.)

4

How to Recover if Attacked:

1. Apply the applicable ‘Fixed Version’ patch to the affected SonicWall product or products and

2.Or Enable administrator/user lockout in the appliance in the 'Administrator' settings of the software.

3. Or reinstall or reboot the software and reset the authenticator app

Low Severity Report

1

Vulnerability Description: A vulnerability in the software of a Cisco Next Generation Firewall could allow an attacker to decrypt messages and eavesdrop on the network.

This type of attack is known as a “Chosen-Ciphertext Attack” (CCA)

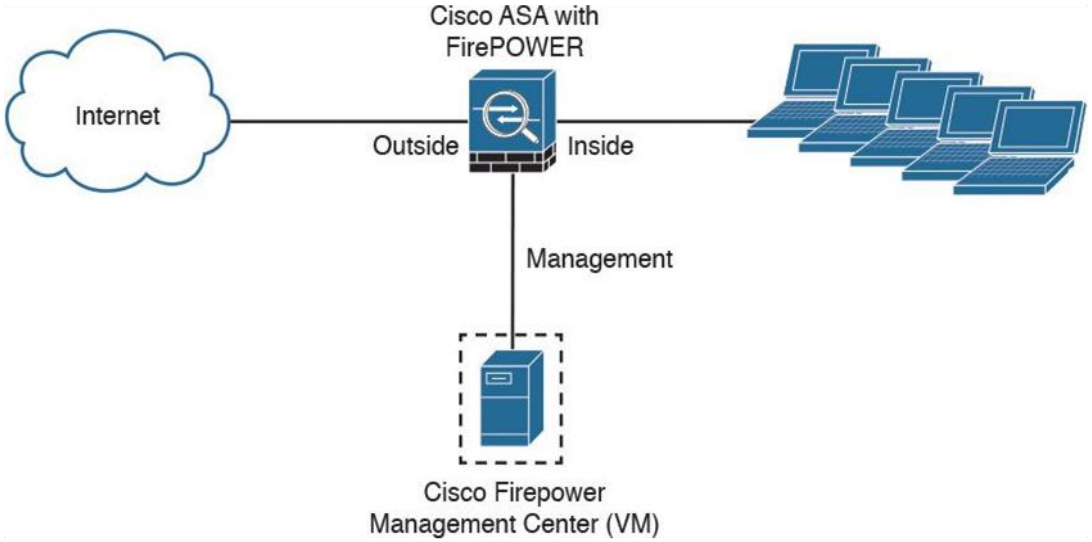
The attacker will send known cyphertexts into the vulnerable system to obtain the resulting plaintexts.

From that information, the attacker will attempt to recover the key used for decryption.

Once the key is recovered, the attacker can eavesdrop on the network and read encrypted traffic.

The Chosen-Ciphertext attack is almost always associated with public key cryptosystems.

2



Low Severity Report

3

How to Prevent this Type of Attack:

Download and Install the Cisco software update that addresses the vulnerability.

Do not provide an “Oracle” to the attackers.

Additional suggestion is to consider a more secure type of cryptography other than RSA. Possibly Elliptical Curve.

4

How to Recover if Attacked:

The first step is to restore factory settings on the Cisco Appliance and reset passwords.

Review Firewall logs to see if any unusual activity.

If there is any unusual activity, review all network system logs for signs of further penetration.

Update all software patches and run Anti-Virus scan of the entire system.

Thanks so much for attending!

Any Questions?

References

Critical Vulnerability

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41924
https://github.com/tailscale/tailscale/security/advisories/GHSA-vqp6-rc3h-83cp
https://emily.id.au/tailscale
https://tailscale.com/security-bulletins/#ts-2022-004

High Vulnerability

National Vulnerability Database "CVE-2020-3133 Detail" https://nvd.nist.gov/vuln/detail/CVE-2020-3133#range-6004928
Torres, Rolando "How to Protect Your Business from Phishing Attacks" ABACODE https://abacode.com/how-to-protect-your-business-from-phishing-attacks/#
Hawthorn, Trevor "14 Things to Do After a Phishing Attack" Proofpoint https://www.proofpoint.com/us/security-awareness/post/14-things-do-after-phishing-attack

Medium Vulnerability

https://www.reddit.com/r/blueteamsec/comments/11jtntu/sonicos_sslvpn_improper_restriction_of_excessive/
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005
https://en.wikipedia.org/wiki/Multi-factor_authentication
https://www.google.com/search?q=captcha+meaning&rlz=1C1JZAP_enUS958US958&oq=CAPTCHA&aqs=chrome.2.0i67i433j0i67j0i433i512j0i67i131i433j0i67j0i67i433j0i433i512j0i512l3.1509j0j15&sourceid=chrome&ie=UTF-8
https://cwe.mitre.org/data/definitions/307.html

Low Vulnerability

National Vulnerability Database "Detail CVE-2020-3585" https://nvd.nist.gov/vuln/detail/CVE-2020-3585
Firmino, Luiz "Chosen-Ciphertext Attack (CCA)" Linkedin Pulse https://www.linkedin.com/pulse/20141201173411-1571978-chosen-ciphertext-attack-cca/
Security Stack Exchange Users ""Best protection against a Chosen-Ciphertext Attack" Security Stack Exchange https://security.stackexchange.com/questions/9781/best-protection-against-a-chosen-ciphertext-attack
PIE Staff "Protecting RSA based Protocols Against Adaptive Chosen-Ciphertext Attacks" Paragon Initiative https://paragonie.com/blog/2018/04/protecting-rsa-based-protocols-against-adaptive-chosen-ciphertext-attacks