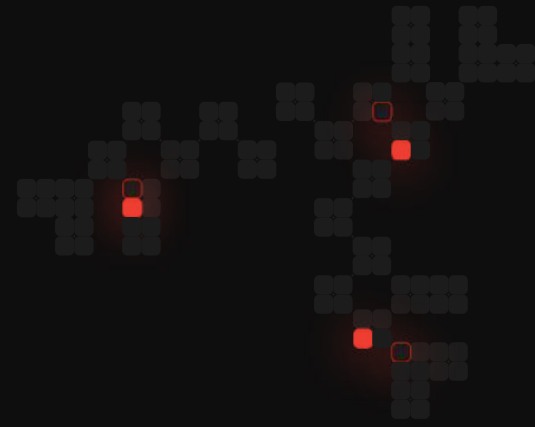


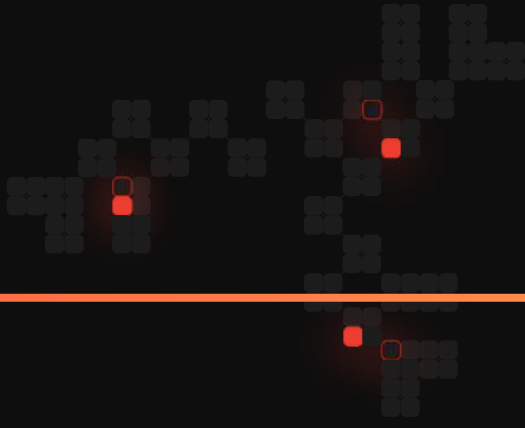


CASE **STUDY**

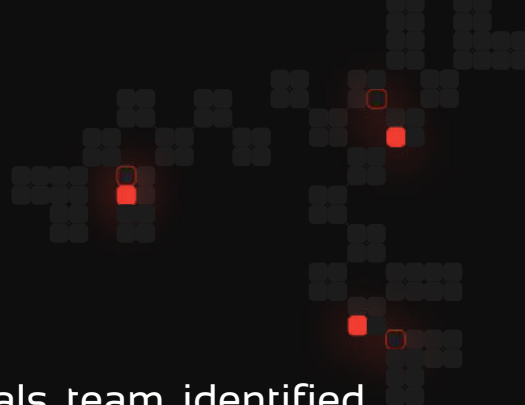
**CYBER HEALS PREVENTED A
GOVERNMENT OIL COMPANY
FROM CRITICAL VULNERABILITIES**



CONTENTS



Overview		3
Our quest for security assessment		3
What is CISCO ASA Firewall?		4
Discovery and Impact		4
Unearthing the vulnerabilities		5
Implications for network security		8
Stay vigilant and proactive		8
Conclusion		9



Overview

During the penetration testing, the Cyber Heals team identified an LFI and XSS vulnerability in Cisco ASA Firewall. Firewalls are often hailed as the unsung heroes of network security, standing as the first line of defense against cyber threats. However, what happens when these guardians themselves become vulnerable to exploitation?

Our quest for security assessment

Our exploration of the Cisco ASA Firewall started with a commitment to rigorously test a company for its defenses. Our team's dedication to ensuring the robustness of cyber security fueled our journey towards uncovering vulnerabilities that posed significant risks to the integrity of the firewall.

What is CISCO ASA Firewall?

The Cisco ASA Software offers enterprise-level firewall capabilities across a range of devices, from standalone appliances to virtual setups. Its feature-rich offerings include Integrated IPS, VPN, and Unified Communications features, as well as multi-site clustering and high availability for critical applications. Context awareness, supported by technologies like Cisco TrustSec, adds an extra layer of security to the network. Context awareness with Cisco TrustSec and identity-based firewall Support for dynamic routing and per-context site-to-site VPN.

Discovery and Impact:

Our quest to assess the security posture of Cisco ASA Firewall led us down a path of rigorous recon and testing. Through this process, we unearthed two significant vulnerabilities: Local File Inclusion (LFI) and Cross-Site Scripting (XSS). These vulnerabilities, identified as CVE-2020-3452 and CVE-2020-3580, pose substantial risks to the integrity and security of the firewall.

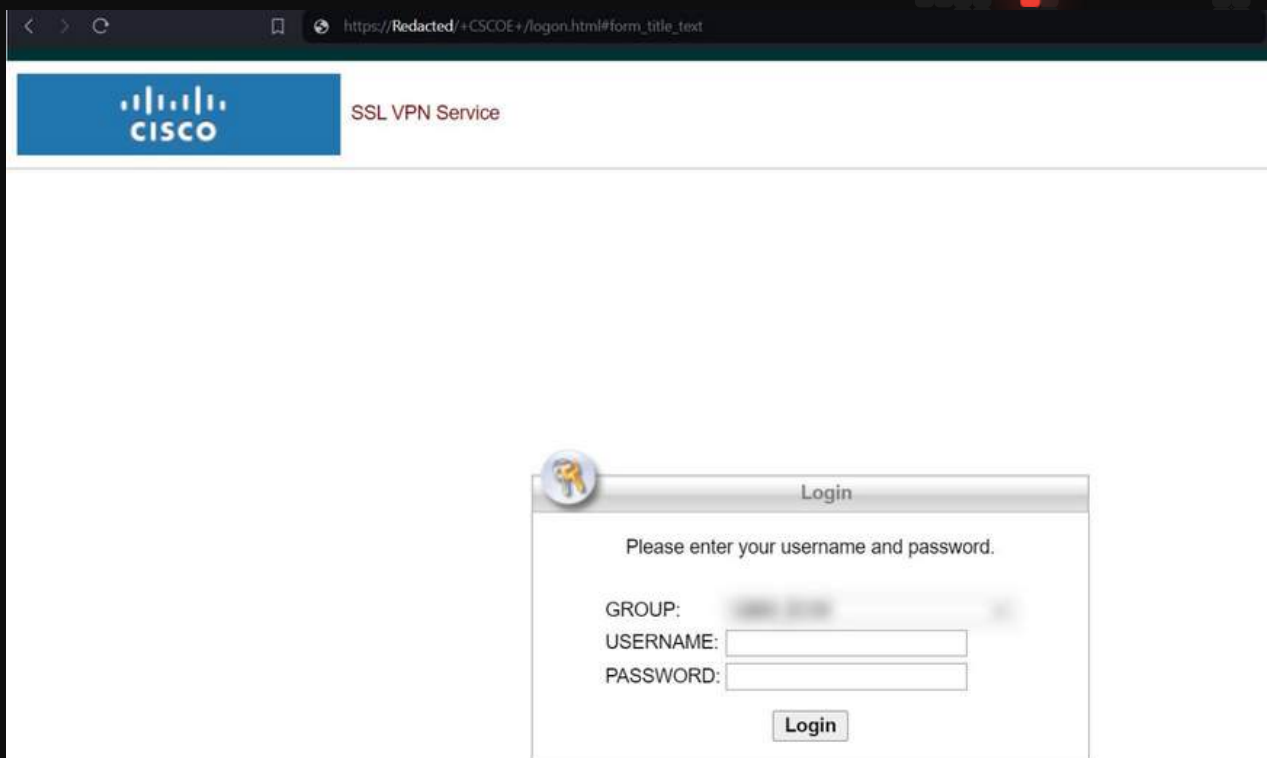


Image 1: shows vulnerable cisco ssl vpn service

Unearthing the vulnerabilities

Through meticulous research and exhaustive testing, we stumbled upon two key vulnerabilities within the Cisco ASA Firewall: Local File Inclusion (LFI) and Cross-Site Scripting (XSS). These vulnerabilities, identified as CVE-2020-3452 and CVE-2020-3580, raised alarm bells due to their potential to compromise the security and confidentiality of the firewall.

CVE-2020-3452 (LFI)

Local File Inclusion (LFI) vulnerability: This vulnerability allows an attacker to access sensitive files stored on the firewall, potentially leading to unauthorized disclosure of critical information.

For example, to read: `"/+CSCOE+/portal_inc.lua"` file.

You will enter as

```
https://redacted/+CSCOT+/translation-table?  
type=mst&textdomain=/%2bCSCOE%2b/portal_inc.lua&default-  
language&lang=../
```

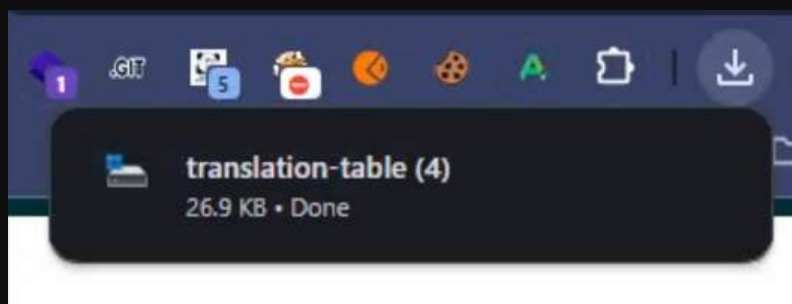


Image 2: Successful local file inclusion leads to sensitive file disclosure

CVE-2020-3580 (XSS)

Cross-Site Scripting (XSS) vulnerability: With this vulnerability, malicious actors can inject harmful scripts into web pages viewed by other users, paving the way for various attacks such as session hijacking or defacement.



Image 3: Requesting with xss payload in SAMLResponse parameter

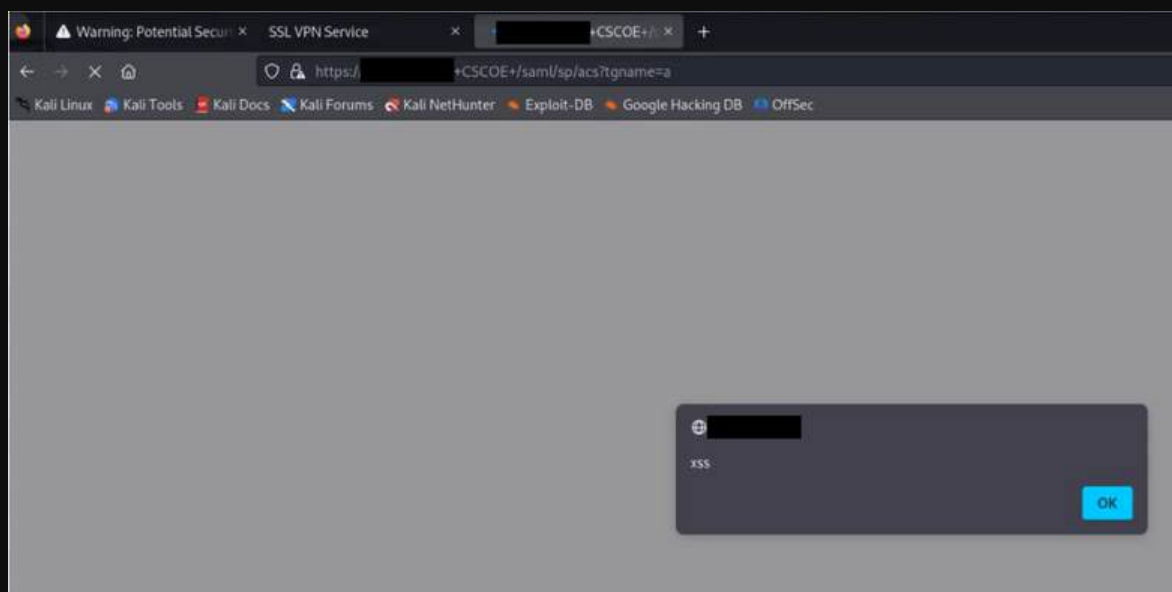


Image 4: the xss is triggered

Implications for network security

The discovery of these vulnerabilities underscored the importance of timely patching and proactive security measures to safeguard against potential exploits. The fallout from a successful attack exploiting these vulnerabilities could be catastrophic, resulting in data breaches, service disruptions, and reputational damage for organizations relying on the Cisco ASA Firewall for protection.

Stay vigilant and proactive

In a landscape where cyber threats evolve at a breakneck pace, staying ahead of vulnerabilities is crucial. Regular security assessments, prompt patching of known vulnerabilities, and a proactive stance towards cybersecurity are key to fortifying the defenses of critical network infrastructure like the Government Oil company.

Conclusion

As we conclude our journey through the realms of cybersecurity, the lessons learned from our encounter with the vulnerabilities in the Oil Company serve as a stark reminder of the ongoing battle against cyber threats. Let us harness this knowledge to bolster our security posture, ensuring that our networks remain resilient in the face of adversities. Remember, vigilance is our greatest ally in the fight for a secure digital future.

Remember, in the intricate dance of cybersecurity, knowledge is power, and vigilance is our shield. Let's band together to fortify our defenses and avoid vulnerabilities that threaten the very fabric of our digital world.

**To get the free security assessment:
<https://cyberheals.com/free-pentest>**