Ex160

Joshua Main-Smith

2020-12-13

Contents

Executive Summary **4**
- Background . . . 4
- Overall Posture . . . 4
- Risk Ranking/Profile . . . 4
- General Findings . . . 5
- Recommendation Summary . . . 5
- Strategic Roadmap . . . 5

Technical Report **6**
- Finding: Misconfigured Network . . . 6
  - Risk Rating: Medium – DREAD Score 4+8+3+3+4 = 22 . . . 6
  - Vulnerability Description . . . 6
  - Confirmation method . . . 6
  - Mitigation or Resolution Strategy . . . 6
- Finding: Backdoor Vulnerability . . . 6
  - Risk Rating: High – DREAD Score 8+9+10+7+7 = 43 . . . 6
  - Vulnerability Description . . . 7
  - Confirmation method . . . 7
  - Mitigation or Resolution Strategy . . . 7
- Finding: Anonymous FTP Login . . . 7
  - Risk Rating: Medium – DREAD Score 4+8+4+2+8 = 26 . . . 7
  - Vulnerability Description . . . 7
  - Confirmation method . . . 7
  - Mitigation or Resolution Strategy . . . 7
- Finding: FTP Unencrypted Cleartext Login . . . 7
  - Risk Rating: Medium – DREAD Score 6+4+5+7+4 = 26 . . . 7
  - Vulnerability Description . . . 8
  - Confirmation method . . . 8
  - Mitigation or Resolution Strategy . . . 8
  - Vulnerability Description . . . 8
- Finding: Stack Buffer Overflow . . . 8
  - Risk Rating: Medium – DREAD Score 7+8+8+3+5 = 31 . . . 8

Vulnerability Description . . . 8
Confirmation method . . . 8
Mitigation or Resolution Strategy . . . 9
Finding: Default Router Credentials Used . . . 9
Risk Assessment: High – DREAD Score 10+10+8+8+6 = 42 . . . 9
Vulnerability Description . . . 9
Confirmation method . . . 9
Mitigation or Resolution Strategy . . . 9
Finding: Users can Create Local Admin Accounts . . . 9
Risk Assessment: High – DREAD Score 10+7+8+7+5 = 37 . . . 9
Vulnerability Description . . . 9
Confirmation method . . . 9
Mitigation or Resolution Strategy . . . 10
Finding: Hyperlinks to Sensitive Data . . . 10
Risk Assessment: Medium – DREAD Score 6+8+5+3+6 = 28 . . . 10
Vulnerability Description . . . 10
Confirmation method . . . 10
Mitigation or Resolution Strategy . . . 10
Finding: Remote Desktop Open on Patronum . . . 10
Risk Assessment: Medium – DREAD Score 3+8+5+5+4 = 25 . . . 10
Vulnerability Description . . . 10
Confirmation method . . . 11
Mitigation or Resolution Strategy . . . 11
Finding: Plaintext Passwords Found on Patronum . . . 11
Risk Assessment: High – DREAD Score 10+7+9+8+6 = 40 . . . 11
Vulnerability Description . . . 11
Confirmation method . . . 11
Mitigation or Resolution Strategy . . . 11
Finding: HTTP Landing Page . . . 11
Risk Assessment: Medium – DREAD Score 3+6+7+3+6 = 25 . . . 11
Vulnerability Description . . . 11
Confirmation method . . . 12
Mitigation or Resolution Strategy . . . 12
Finding: Outdated Sudo Program . . . 12
Risk Assessment: High – DREAD Score 9+8+10+8+6 = 41 . . . 12
Vulnerability Description . . . 12
Confirmation method . . . 12
Mitigation or Resolution Strategy . . . 12
Finding: Users Signing into Fictitious Authentication Box . . . 12
Risk Assessment: Medium – DREAD Score 10+6+9+6+4 = 35 . . . 12
Vulnerability Description . . . 13
Confirmation method . . . 13
Mitigation or Resolution Strategy . . . 13
Finding: Users Navigating to Outside Websites with Company Resources . . . 13
Risk Assessment: Medium – DREAD Score 6+4+8+4+2 = 24 . . . 13

Vulnerability Description 13
Confirmation method 13
Mitigation or Resolution Strategy 14
Finding: Client Side File Extension Check 14
Risk Assessment: High – DREAD Score 10+8+8+7+7 = 40 14
Vulnerability Description 14
Confirmation method 14
Mitigation or Resolution Strategy 14
Finding: Sensitive Data Exfiltrated 14
Risk Assessment: High – DREAD Score 8+8+8+6+7 = 37 14
Vulnerability Description 14
Confirmation method 15
Mitigation or Resolution Strategy 15
Finding: CVE-2017-0143 15
Risk Assessment: High – DREAD Score 10+8+10+10+9 = 47 . . 15
Vulnerability Description 15
Confirmation method 15
Mitigation or Resolution Strategy 15

Executive Summary

Background

Back in September, Matt Mason had requested our services in testing various aspects of F4rmC0rp security. We were authorized to test the security of their network services, with an IP block of 172.30.0.0/24 with the home papge being 172.30.0.128:80.

During the course of our analysis, we tested various aspects of F4rmC0rp's security. which included a vulnerability and exploitability assessment. A DREAD score was assigned to each finding listed below, with scores between 5-19 ranked as low, 20-35 as medium, and 36-50 as high. It is suggested to resolve issues ranked high and medium immediately. Low ranking issues can be resolved when it's most convenient.

Overall Posture

There were several vulnerabilities and exploits that we had discovered during the course of our analysis, with the most important to note being those vulnerabilities that lead to us gaining root privileges on several machines.

Of particular concern are the instances where several users are affected, such as with the newly deployed backup Domain Controller running on F4rmc0rp's network. Escalating our privileges to administrator here let us have complete control over the whole domain, an issue that could have catastrophic consequences if an attacker were to gain control of such a system.

Overall, we were able to acquire root access the majority of machines we gained access to putting F4rmC0rp at risk for sensitive data exfiltration and to leave the company at the whims of a potential attacker. For this reason, we ranked F4rmC0rp at high risk to exploitation.

Risk Ranking/Profile

Risk ranking can be determined from the damage an exploit would have if it were to occur by the likelihood of it occurring. The damage that would occur from several of the machines we tested has lead us to escalating our privileges to root. Further, we were able to gain access to the primary and beta Domain Controllers, giving us administrative control over all users in the domain. As such, the risk F4rmC0rp faces can be catastrophic.

The likelihood of an attacker taking advantage of these vulnerabilities are also very high. This is due to many of these vulnerabilities being found by a simple vulnerability scan. Several vulnerabilities can be exploited by low information attackers due to several of the vulnerabilities having commonly known

exploits, implemented in well known Metasploit modules.

Overall, F4rmC0rp is at high risk of exploitation from even low information attackers.

General Findings

There were several services that were vulnerable to exploitation simply due to outdated and unpatched software. These vulnerable services were easily found by running vulnerability scripts or by researching the software version.

There were also a few instances where Brian Oppenheimer created a custom service, running this service on the F4rmC0rp network. One of these services allowed us to explore the www.f4rmc0rp.com machine as Brian due to a buffer overflow vulnerability. Another service allowed us to upload a malicious PHP file to the F4rmC0rp machine, allowing us to explore the machine as www-data.

Additionally, there were a few social engineering attacks successfully employed during the course of analysis. Such attacks included one employee visiting a page outside the company network with a F4rmC0rp machine to a website we set up containing a malicious script. Another instance was an employee using their credentials to sign into a fictitious sign in box.

Recommendation Summary

Overall, F4rmC0rp would be best served by issueing regular software updates and patches for the services running on the network. This would eliminate several of the exploits we were able to employ. It is also of the utmost importance to remove innerouter from being accessible on WAN and to change the default login credentials. Having access to innerouter allowed us to explore several LAN machines that would have otherwise been inaccessible.

We also recommend for employees to not use custom software unless it's absolutely necessary. Unless the employee has been trained to make secure software, there will very likely be oversights in the construction of an application. Further, it is highly recommended to require user authentication when logging into a service.

Lastly, we recommend social engineering and security training for the employees. This would mitigate some common pitfalls attackers typically use.

Strategic Roadmap

To ensure continued security, it is recommended to do regular vulnerability scanning against all the service running on F4rmC0rp. Even something that

seems very small can lead to huge payoffs.

Regular security training for the employees is recommended to encourage continued diligence against attackers and to encourage reporting suspicious behavior. Performing regular penetration tests would also ensure continued security as more services, employees, software, etc. are typically added over the course of the company lifetime.

Technical Report

Finding: Misconfigured Network

Risk Rating: Medium – DREAD Score 4+8+3+3+4 = 22

A misconfigured network could be subject to a subdomain takeover and used as a pivot point for other hosts for interested parties in gaining access to sensitive information, if not already present on the initial one.

Vulnerability Description

There is a potential misconfigured network that is leaking an internal address space. Particularly, KEY005-IHIHIWJRhzMTH4qXCCwOuA.f4rmc0rp.com. This could be due to forgetting to configure or deregister from a 3rd party server.

Confirmation method

This can be confirmed by running a **fierce** scan on **f4rmc0rp.com**. Using a wordlist generated from scanning the host along with a typical host wordlist would generate the same results. Or, more easily, **fierce -dns f4rmc0r.com -wide**.

Mitigation or Resolution Strategy

Properly configure the subdomains on the network to not leak subdomains not intended for the general public.

Finding: Backdoor Vulnerability

Risk Rating: High – DREAD Score 8+9+10+7+7 = 43

The risk of running this service is an attacker can use a specially crafted payload to bypass authentication to gain access to the system. This puts the machine at risk for sensitive data being exfiltrated.

Vulnerability Description

Allows an attacker to execute arbitrary code in a backdoor attack. Originally, TCP port 6200 was seen to be closed when running an nmap scan. But, after applying known attack credentials associated with a known vulnerability regarding vsptd 2.3.4 on port 2121, port 6200 was toggled open. Netcat can then be used to connect to the new listening port.

Confirmation method

This can be confirmed by running a vulnerability scan against port 2121 on 172.30.0.128. This will reveal a vulnerable version of FTP running.

Mitigation or Resolution Strategy

This can be mitigated by updating to the most recent version of vsftpd.

Finding: Anonymous FTP Login

Risk Rating: Medium – DREAD Score 4+8+4+2+8 = 26

The general public has the option to log in as an anonymous user. A possible consequence of this is an attacker viewing sensitive information.

Vulnerability Description

Users can login into the FTP service without providing credentials as an anonymous user. This opens the possibility of an attacker reading files unintended for the general public.

Confirmation method

This can be confirmed by logging in as user anonymous without providing a password. Further, a vulnerability scanner can confirm this vulnerability present.

Mitigation or Resolution Strategy

Configure the service to not allow anonymous logins.

Finding: FTP Unencrypted Cleartext Login

Risk Rating: Medium – DREAD Score 6+4+5+7+4 = 26

The FTP service is at risk of a man in the middle attack. An attacker is able to capture traffic in cleartext, potentially gaining user credentials.

Vulnerability Description

Allows attackers to sniff traffic between user and host in recovering login credentials because the traffic is in cleartext.

Confirmation method

This can be confirmed by running a network traffic sniffer (such as Wireshark) and viewing the traffic as a user logs in. Further, a vulnerability scanner will typically detect this (such as OpenVAS).

Mitigation or Resolution Strategy

This can be mitigated by encrypting all traffic between user and host.

Vulnerability Description

Using OpenVAS to scan for any vulnerabilities on www.f4rmc0rp.com (172.30.0.128), we found that there are two high, two medium, and one low ranking vulnerabilities. A screenshot of the vulnerabilities found can be seen below.

Finding: Stack Buffer Overflow

Risk Rating: Medium – DREAD Score 7+8+8+3+5 = 31

The service employed here is vulnerable to a buffer overflow attack. An attacker exploiting this vulnerability allows the use of arbitrary Linux commands to be executed as whichever user is signed in.

Vulnerability Description

The new service that Brian Oppenheimer has deployed is vulnerable to a buffer overflow attack. Entering 32 bytes of characters into the username field followed by arbitrary shell commands overwrites the populated commands buffer implemented by Oppenheimer's service.

Confirmation method

Connecting to Brian's service on 172.30.0.128:1337 with Netcat will prompt the user for a username. Inputting the username field with 32 bytes of characters followed by the path to a desired command (such as **/bin/bash**) will make that command available when logging in as a user, such as brian.

Mitigation or Resolution Strategy

This can be mitigated by adding a field of authentication, such as a password, employing proper user input sanitization. Additionally, this could further be mitigated by populating the commands after the user has signed in and to sanitize any input that a potential attacker may employ.

Finding: Default Router Credentials Used

Risk Assessment: High – DREAD Score 10+10+8+8+6 = 42

With the PfSense router containing the default login credentials and it being open to the wide area network gives an attacker control over packets passing through the router.

Vulnerability Description

The company router uses the default login credentials and is reachable to those outside the network.

Confirmation method

This can be confirmed by navigating to https://172.30.0.3 and logging in with the default login credentials provided by PfSense.

Mitigation or Resolution Strategy

This issue can be resolved by changing the default login credentials and removing the router from being available on the wide area network.

Finding: Users can Create Local Admin Accounts

Risk Assessment: High – DREAD Score 10+7+8+7+5 = 37

Users without admin privileges are able to create a local admin account, thereby bypassing the security impediments put into place for the said user by signing in as a user with admin privileges.

Vulnerability Description

The vulnerability is due to a misconfiguration of the system that allows users without admin privileges to create local admin accounts.

Confirmation method

This can be confirmed by utilizing the PowerUp Powershell script by running the **Invoke-AllChecks** option. This will scan the system for misconfigurations that can be abused by an attacker.

Mitigation or Resolution Strategy

Reconfigure functionality that allows non-admin users to create local admin accounts.

Finding: Hyperlinks to Sensitive Data

Risk Assessment: Medium – DREAD Score 6+8+5+3+6 = 28

A commented out hyperlink to a directory was found in the page source of the web page on **45.79.140.13:80**. Access to the directory was password protected, indicating the presence of sensitive information. Exploitation could lead attackers in viewing or exfiltrating said sensitive information.

Vulnerability Description

Viewing the page source of **45.79.140.13:80** shows the pathway to a directory that has been commented out. Attackers having in possession of the proper credentials can connect to the directory.

Confirmation method

This can be confirmed by navigating to **45.79.140.13:80** and viewing the page source. At the bottom, there's a commented out html hyperlink tag leading to Nomen's Directory. Navigating to the listed directory prompts the user for credentials.

Mitigation or Resolution Strategy

If the pathway to the directory isn't intended for public knowledge, then the hyperlink should be deleted rather than commented out.

Finding: Remote Desktop Open on Patronum

Risk Assessment: Medium – DREAD Score 3+8+5+5+4 = 25

Those who do have access to the Patronum machine can access it via RDP. Someone who should not have access to the machine can access it and log in as a user if an attacker has possession of user credentials.

Vulnerability Description

Remote desktop is listening for incoming local connections. Connection remotely may be convenient, but it leaves an avenue for a potential attacker to abuse this functionality by logging in with previously acquired credentials or attempt to brute force username/password combinations.

Confirmation method

This can be confirmed by viewing which services are running on their respective port. Remote desktop typically runs on port 3389, which was the case for Patronum.

Mitigation or Resolution Strategy

Unless MS RDP is absolutely necessary, port 3389 should be closed to any incoming connection.

Finding: Plaintext Passwords Found on Patronum

Risk Assessment: High – DREAD Score 10+7+9+8+6 = 40

Username and password combinations were found on Patronum in plaintext under one or more user accounts. These can be seen by any user who has access as a local administrator.

Vulnerability Description

Unencrypted username/password combinations can easily be seen by anyone who has proper administrator privileges.

Confirmation method

This can be confirmed by navigating to the Desktop folders of m.mason and m.mason.F$RMC0RP and viewing the text files containing plaintext user/admin credentials.

Mitigation or Resolution Strategy

Don't store plaintext passwords.

Finding: HTTP Landing Page

Risk Assessment: Medium – DREAD Score 3+6+7+3+6 = 25

The webpage www.f4rmc0rp.com uses HTTP as the landing page, then switches to HTTPS upon logging in. An SSLStrip attack can be used to capture packets as a man in the middle attack, potentially gaining access to login credentials.

Vulnerability Description

An SSLStrip attack sits between the browser and a server and logs incoming or outgoing traffic. The attack forces the browser and server to communicate via HTTP, then proxying the information obtained and logged from this with its intended destination.

Confirmation method

This can be confirmed by navigating to the home page using both the http and https protocols. If both protocols can be reached, then the service is vulnerable to a man in the middle attack.

Mitigation or Resolution Strategy

Use a security policy that requires communication only through HTTPS. One solution HTTP Strict Transport Security (HSTS), which is a policy that demands machines only communicate via HTTPS.

Finding: Outdated Sudo Program

Risk Assessment: High – DREAD Score 9+8+10+8+6 = 41

Devbox is running an outdated version of sudo that is vulnerable to an integer error allowing the user m.mason to run as root when executed.

Vulnerability Description

Sudo doesn't check for the existence of a user when given its ID. When **-1** is selected as the user ID, **0** is returned (the ID for root). Running **sudo -u-1 command** gives m.mason root access to the command the user is allowed to run. If the version is 1.8.27 or below, the machine is still vulnerable to this exploit. Further, this exploit works in conjunction with the particular syntax in the **/etc/sudoers** file. Namely, if a user has the syntax **user ALL=(ALL,!root) /bin/program** and a vulnerable version of sudo is running then the machine is vulnerable to the exploit.

Confirmation method

This can be confirmed by checking the version of sudo running on the machine with **sudo -V**. This is in conjunction with the syntax of the **sudoers** file mentioned above.

Mitigation or Resolution Strategy

Update **sudo** to the newest version.

Finding: Users Signing into Fictitious Authentication Box

Risk Assessment: Medium – DREAD Score 10+6+9+6+4 = 35

Users entered their credentials into a fictitious authentication box generated from Responder. The consequence of this is an attacker could acquire user credentials that could be used to sign into systems, gaining access to sensitive information.

Vulnerability Description

Responder generates a fake authentication box and forces the user to sign in with their credentials. These credentials are forwarded to the attacker using basic authentication, granting an attacker access to sensitive information.

Confirmation method

Regular vulnerability and exploitation assessments would be necessary in confirming the persistence of the vulnerability. This would be recommended after the proper mitigation measures have been employed, such as social engineering and security training.

Mitigation or Resolution Strategy

Training for employees in recognising common social engineering attacks.

Finding: Users Navigating to Outside Websites with Company Resources

Risk Assessment: Medium – DREAD Score 6+4+8+4+2 = 24

Users are allowed to use company resources to browse websites outside the company network. A potential consequence of this is private information communicated from the user's browser may be captured by attackers hosting malicious websites.

Vulnerability Description

When a user visits a malicious website, such as the one crafted below in the attack narrative, private information communicated from the browser to the server may be capture by an attacker (such as cookie information). Further, there are a variety of other attacks an attacker may employ to gain further information, such as viewing webcams, html pages, known browser exploits, etc.

Confirmation method

This method can be confirmed by setting up regular vulnerability and exploitation assessments. It is recommended to do this after proper social engineering and security training has been issued to the appropriate employees regarding safe computer practice.

Mitigation or Resolution Strategy

Prevent user's from navigating to unknown web hosts by employing white list rules in the firewall (for example). Additionally, giving the employees social engineering training may prove useful.

Finding: Client Side File Extension Check

Risk Assessment: High – DREAD Score 10+8+8+7+7 = 40

The webpage does a client-side check for a matching accepted file extension. An attacker can manipulate the client side check to get around this. Further, an attacker can fool the file extension checker by appending the file with the required file extension, allowing an attacker to execute arbitrary code.

Vulnerability Description

With client-side checks, a user/attacker has control over how the code operates. Then, an attacker can capture and manipulate that traffic before it's sent out to upload the desired file, given there is no server-side check.

Confirmation method

This can be confirmed by uploading any file by first appending the file with the required file extension (.png, .PNG, .jpg, .JPG). If successful, the service would be vulnerable to a PHP injection attack.

Mitigation or Resolution Strategy

Only do server-side checks for authentication procedures, limiting the control flow a user/attacker has. Further, don't trust file extensions. Rather, check file contents for indicators that it is the required file.

Finding: Sensitive Data Exfiltrated

Risk Assessment: High – DREAD Score 8+8+8+6+7 = 37

User credentials were exfiltrated by doing a simple string search for key information.The consequence of this is an attacker can gain access to the user account after recovering credentials.

Vulnerability Description

After decompiling the application an attacker was easily able to see the functionality of the app by viewing the source code, as it was not obfuscated. An attacker can view sensitive information as the data was not properly handled.

Confirmation method

This can be confirmed by doing a string search with **jadx-gui** for a username or password. Finding the Base64 encrypted username and password can be easily decrypted using **echo encryptedText | base64 -d**.

Mitigation or Resolution Strategy

Follow the OWASP Mobile Application Security Verification Standard to implement Resiliency Against Reverse Engineering and Tampering (MASVS-R).

Finding: CVE-2017-0143

Risk Assessment: High – DREAD Score 10+8+10+10+9 = 47

The BDC host is vulnerable to CVE-2017-0143 (Eternal Blue), allowing an attacker to perform remote code execution through the server message block. An attacker can perform actions as NT Authority system, such as creating users with administrator credentials, overriding passwords, viewing the file system, and anything else that's allowed by a user with administrative privileges.

Vulnerability Description

Eternal Blue takes advantage of a vulnerability in the Server Message Block 1.0 (SMBv1) from a mishandling of specially crafted packet requests issued by attackers (Source).

Confirmation method

To confirm that this vulnerability still exists, run a vulnarability scan against BDC (such as with Nmap). It is recommended to use the **–script vuln** script with Nmap. Another option is with Metasploit's **auxiliary/smb/smb_ms17_010** module. This will scan BDC and determine if it is likely vulnerable to MS17-010.

Mitigation or Resolution Strategy

Issue a patch to Windows Server 2008 on BDC to run the most updated version.