Prerequisites

- **Administrative Access**: Ensure you have admin rights on the server.
- **Remote Desktop Access**: Make sure Remote Desktop is enabled and you can log in.
- **Stable Internet Connection**: Needed for downloading patches.
- **Backup**: It's a good idea to back up your server before making changes.

Accessing the Server via Remote Desktop

1. **Open Remote Desktop Connection on Your Local Machine**:
    - Press `Windows Key + R` to open the Run dialog.
    - Type `mstsc` and press **Enter**.
2. **Connect to the Server**:
    - Enter your server's **IP address** or **hostname**.
    - Click **Connect**.
    - Enter your **username** and **password** when prompted.
    - Click **OK**.

Creating the Patch Folder on Desktop

1. **Create "patch" Folder**:
    - After logging into the server, right-click on the **Desktop**.
    - Select **New** > **Folder**.
    - Name the folder **patch**.

---

1. Patching Critical Vulnerabilities (Severity 5)

Vulnerability Count: 2

Vulnerabilities:

1. **CVE-2023-38545**: Curl heap buffer overflow.
2. **Windows OS Vulnerabilities**: Specific KB updates needed.

A. Updating Curl to Fix CVE-2023-38545

Step 1: Verify Current Curl Version

- **Open Command Prompt**:

    - Click **Start**, type `cmd`, right-click on **Command Prompt**, and select **Run as administrator**.

Run Command:
css
Copy code
```
curl --version
```

-
    - Press **Enter**.
    - Note the version displayed.

Step 2: Download Curl 8.4.0 Patch

Download URL:
arduino
Copy code
```
https://curl.se/windows/
```

-
- **Download Steps**:
    - Open **Internet Explorer** or **Edge**.
    - Go to the URL above.
    - Click on **curl for 64-bit** to download.

When prompted, save the file to:
makefile
Copy code
```
C:\Users\YourUsername\Desktop\patch
```

    -
        - Replace **YourUsername** with your actual username.

Step 3: Install Curl 8.4.0

- **Navigate to Patch Folder**:
    - Open **File Explorer**.
    - Go to **Desktop** > **patch**.
- **Extract the ZIP File**:
    - Right-click on the downloaded **curl** ZIP file.
    - Select **Extract All...** and extract to the same folder.
- **Copy curl.exe to System32**:
    - Open the extracted folder.
    - Locate **curl.exe**.
    - Right-click **curl.exe** and select **Copy**.

Navigate to:
makefile
Copy code
```
C:\Windows\System32
```

    -
    - Paste **curl.exe** here.

    - If prompted for administrator permission, click **Continue**.

Step 4: Verify Updated Curl Version

- **Open Command Prompt as Administrator**.

Run Command:
css
Copy code
```
curl --version
```

-
    - Press **Enter**.
    - Confirm the version is now **8.4.0**.

B. Installing Microsoft Security Updates

Updates Needed:

- **KB5040430**
- **KB5040448**

Step 1: Check Current Windows Version
Run Command:
mathematica
Copy code
```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

-
    - Press **Enter**.
    - Note your OS details.

Step 2: Download Security Updates

- **Download URLs**:

KB5040430:
arduino
Copy code
```
https://www.catalog.update.microsoft.com/Search.aspx?q=KB5040430
```

    -

KB5040448:
arduino
Copy code
```
https://www.catalog.update.microsoft.com/Search.aspx?q=KB5040448
```

    -
- **Download Steps**:
    - Open **Internet Explorer** or **Edge**.

    - Go to each URL.
    - Click on the appropriate update matching your OS and system architecture (usually **x64-based Systems**).
    - Click **Download**.
    - In the pop-up window, click the link to download the **.msu** file.

Save the file to:
makefile
Copy code
```
C:\Users\YourUsername\Desktop\patch
```

    -

Step 3: Install Security Updates

- **Navigate to Patch Folder**:
    - Open **File Explorer**.
    - Go to **Desktop** > **patch**.
- **Install KB5040430**:
    - Double-click on the **windows10.0-kb5040430-...x64.msu** file.
    - Follow the installation prompts.
- **Install KB5040448**:
    - Repeat the steps above for **KB5040448**.
- **Restart the Server**:
    - If prompted, restart the server after each installation.

Step 4: Verify Installation

- **Run Command Prompt as Administrator**.

Run Command:
arduino
Copy code
```
wmic qfe list brief | findstr "KB5040430"
```

-
    - Press **Enter**.
    - Ensure the update is listed.

Repeat for KB5040448:
arduino
Copy code
```
wmic qfe list brief | findstr "KB5040448"
```

-
    - Press **Enter**.

---

2. Patching High-Severity Vulnerabilities (Severity 4)

Vulnerability Count: 22

Vulnerabilities:

- Various Windows OS vulnerabilities requiring KB updates.
- Mozilla Firefox vulnerabilities.

A. Installing Additional Windows Security Updates

Updates Needed:

- **KB5040434**
- **KB5040431**
- **KB5033429**

Step 1: Download Updates

- **Download URLs**:

KB5040434:
arduino
Copy code
`https://www.catalog.update.microsoft.com/Search.aspx?q=KB5040434`

  ○

KB5040431:
arduino
Copy code
`https://www.catalog.update.microsoft.com/Search.aspx?q=KB5040431`

  ○

KB5033429:
arduino
Copy code
`https://www.catalog.update.microsoft.com/Search.aspx?q=KB5033429`

  ○

- **Download Steps**:
  - Open **Internet Explorer** or **Edge**.
  - Go to each URL.
  - Download the appropriate **.msu** files for your system.

Save them to:
makefile
Copy code
`C:\Users\YourUsername\Desktop\patch`

  ○

Step 2: Install Updates

- **Navigate to Patch Folder**.
- **Install KB5040434**:
    - Double-click the **.msu** file.
    - Follow prompts.
- **Install KB5040431** and **KB5033429**:
    - Repeat the steps above for each update.
- **Restart the Server**:
    - Restart after installing all updates.

Step 3: Verify Installation

- **Run Command Prompt as Administrator**.

Run Commands:
arduino
Copy code

```
wmic qfe list brief | findstr "KB5040434"
wmic qfe list brief | findstr "KB5040431"
wmic qfe list brief | findstr "KB5033429"
```

-
    - Ensure each update appears in the results.

B. Updating Mozilla Firefox for High-Severity Vulnerabilities

Vulnerabilities Addressed:

- **MFSA2024-29**: CVE-2024-6615
- **MFSA2023-16**: CVE-2023-32211, CVE-2023-32208

Step 1: Check Current Firefox Version

- **Open Firefox**.
- **Go to**:
    - Menu (three horizontal lines) > **Help** > **About Firefox**.
- **Note the Version**.
- **Close Firefox**.

Step 2: Download Firefox Updates

- **Download URLs**:

Firefox 128:
bash
Copy code

```
https://ftp.mozilla.org/pub/firefox/releases/128.0/win64/en-US/Firefox%20Setup%20128.0.exe
```

    -

Firefox 113 (if needed):
bash
Copy code
```
https://ftp.mozilla.org/pub/firefox/releases/113.0/win64/en-US/Firefox%20Setup%20113.0.exe
```

    -

- **Download Steps**:
    - Open **Internet Explorer** or **Edge**.
    - Navigate to the URLs above.

Save the installers to:
makefile
Copy code
```
C:\Users\YourUsername\Desktop\patch
```

    -

Step 3: Install Firefox Updates

- **Navigate to Patch Folder**.
- **Install Firefox 128**:
    - Double-click **Firefox Setup 128.0.exe**.
    - Follow the installation prompts.
- **Note**: Installing the latest version covers previous vulnerabilities.

Step 4: Verify Firefox Version

- **Open Firefox**.
- **Go to**:
    - Menu > **Help** > **About Firefox**.
- **Confirm the Version is 128.0**.
- **Close Firefox**.

---

3. Patching Medium-Severity Vulnerabilities (Severity 3)

Vulnerability Count: 4

Vulnerabilities:

- Mozilla Firefox vulnerabilities related to mixed-content resources and memory safety (e.g., **CVE-2023-6204**).

Updating Firefox to Version 120

Step 1: Download Firefox 120
Download URL:
bash

Copy code
`https://ftp.mozilla.org/pub/firefox/releases/120.0/win64/en-US/Firefox%20Setup%20120.0.exe`

-
- **Download Steps**:
    - Open **Internet Explorer** or **Edge**.
    - Go to the URL.

Save the installer to:
makefile
Copy code
`C:\Users\YourUsername\Desktop\patch`

    -

Step 2: Install Firefox 120

- **Navigate to Patch Folder**.
- **Install Firefox 120**:
    - Double-click **Firefox Setup 120.0.exe**.
    - Follow the installation prompts.
- **Note**: Since you've installed Firefox 128 earlier, this step is already covered.

Step 3: Verify Firefox Version

- **Open Firefox**.
- **Confirm the Version is at least 120.0 or higher**.
- **Close Firefox**.

---

4. Patching Low-Severity Vulnerabilities (Severity 2)

Vulnerability Count: 2

Vulnerabilities:

- Potential information disclosure issues.
- Local configuration updates needed.

A. Review and Install Any Remaining Windows Updates

Step 1: Check for Windows Updates

- **Open Settings**:
    - Click **Start** > **Settings** (gear icon).
- **Navigate to Update & Security**.
- **Click Check for updates**.
- **Install Any Available Updates**.

- **Restart the Server** if prompted.

Step 2: Verify All Updates are Installed

- **Run Command Prompt as Administrator**.

Run Command:
lua
Copy code
```
wmic qfe list brief /format:table
```

-
    - Review the list to ensure no updates are pending.

B. Update Security Policies: Disable Curl Execution with WDAC

Note: Disabling Curl may impact applications that rely on it. Proceed if you're certain it's safe to disable.

Step 1: Open PowerShell as Administrator

- **Click Start**, type `PowerShell`, right-click **Windows PowerShell**, select **Run as administrator**.

Step 2: Create a WDAC Policy to Block Curl
Create Policy Folder:
arduino
Copy code
```
mkdir C:\Users\YourUsername\Desktop\patch\WDAC_Policies
```

-

Navigate to Policy Folder:
bash
Copy code
```
cd C:\Users\YourUsername\Desktop\patch\WDAC_Policies
```

-

Step 3: Generate Base Policy
Run Command:
mathematica
Copy code
```
New-CIPolicy -Level FileName -FilePath
"C:\Users\YourUsername\Desktop\patch\WDAC_Policies\Policy.xml"
```

-
- **Note**: If `New-CIPolicy` is not recognized, you need to install the **Windows Defender Application Control** feature.

Step 4: Edit Policy to Deny Curl

Open Policy in Notepad:
arduino
Copy code
```
notepad "C:\Users\YourUsername\Desktop\patch\WDAC_Policies\Policy.xml"
```

-
- **Add Deny Rule**:
    - Find the `<Policies>` section.

Add:
xml
Copy code
```
<FileRules>
  <FileRule Id="DenyCurl" Name="Deny Curl Execution" Action="Deny">
    <FileName>curl.exe</FileName>
  </FileRule>
</FileRules>
```

    -
- **Save and Close**.

Step 5: Convert Policy to Binary
Run Command:
objectivec
Copy code
```
ConvertFrom-CIPolicy -XmlFilePath
"C:\Users\YourUsername\Desktop\patch\WDAC_Policies\Policy.xml"
-BinaryFilePath
"C:\Users\YourUsername\Desktop\patch\WDAC_Policies\SIPolicy.p7b"
```

-

Step 6: Deploy the Policy
Copy Policy File:
mathematica
Copy code
```
Copy-Item -Path
"C:\Users\YourUsername\Desktop\patch\WDAC_Policies\SIPolicy.p7b" -Destination
"C:\Windows\System32\CodeIntegrity\SIPolicy.p7b"
```

-
- **Restart the Server**:
    - Close all applications.
    - Restart the server to apply the policy.

Step 7: Verify Curl is Blocked

- **Open Command Prompt**.

Run Command:
css

Copy code
```
curl --version
```

-
    - Press **Enter**.
- **Expected Result**:
    - You should receive an error indicating access is denied.

---

5. Validation and Testing

A. Verify All Installed Updates

- **Run Command Prompt as Administrator**.

Run Command:
lua
Copy code
```
wmic qfe list brief /format:table
```

-
- **Review**:
    - Ensure all the KB updates installed earlier are listed.

B. Check System Functionality

- **Test Applications**:
    - Open commonly used applications to ensure they work.
- **Test Services**:
    - Press `Windows Key + R`, type `services.msc`, press **Enter**.
    - Check that critical services are running.

C. Check Event Logs for Errors

- **Open Event Viewer**:
    - Press `Windows Key + R`, type `eventvwr`, press **Enter**.
- **Review Logs**:
    - Expand **Windows Logs**.
    - Check **Application** and **System** logs for errors.

D. Verify Firefox Functionality

- **Open Firefox**.
- **Browse Websites**:
    - Navigate to several websites to ensure they load properly.
- **Check Add-ons**:
    - Ensure extensions are functioning.

E. Verify Curl is Blocked

- **Open Command Prompt**.

Run Command:
arduino
Copy code
```
curl https://www.google.com
```

-
    - Press **Enter**.
- **Expected Result**:
    - Access should be denied or an error message displayed.

Summary of Actions

- **Total Patches Applied**: 30 vulnerabilities addressed.
- **Windows Updates Installed**:
    - **KB5040430**
    - **KB5040448**
    - **KB5040434**
    - **KB5040431**
    - **KB5033429**
    - Any additional updates found during Windows Update.
- **Applications Updated**:
    - **Curl** updated to version **8.4.0**.
    - **Mozilla Firefox** updated to version **128.0**.
- **Security Policies Enforced**:
    - **WDAC policy** implemented to block **curl.exe** execution.

Additional Recommendations

- **Enable Automatic Updates**:
    - Consider enabling automatic updates for Windows and applications to stay up-to-date.
- **Regular Backups**:
    - Schedule regular backups to prevent data loss.
- **Security Awareness**:
    - Keep informed about new vulnerabilities relevant to your system.
- **Documentation**:
    - Maintain a log of updates and changes made to the server.

Troubleshooting

- **If Updates Fail to Install**:
    - Ensure the system date and time are correct.
    - Check for sufficient disk space.

    - Disable antivirus temporarily if it's blocking installations.
- **If Applications Don't Work After Updates**:
    - Try repairing or reinstalling the application.
    - Check compatibility with the new updates.

Frequently Used Commands

Check Installed Updates:
lua
Copy code
```
wmic qfe list brief /format:table
```

-

Check Windows Version:
mathematica
Copy code
```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

-

Check Curl Version:
css
Copy code
```
curl --version
```

-
- **Check Firefox Version**:
    - Open Firefox, go to **Menu** > **Help** > **About Firefox**.