# Threat Model

# Notepad (Windows 10)

AJ Downey
Joshua Barbee
Wei Wei Chien

11 November 2022

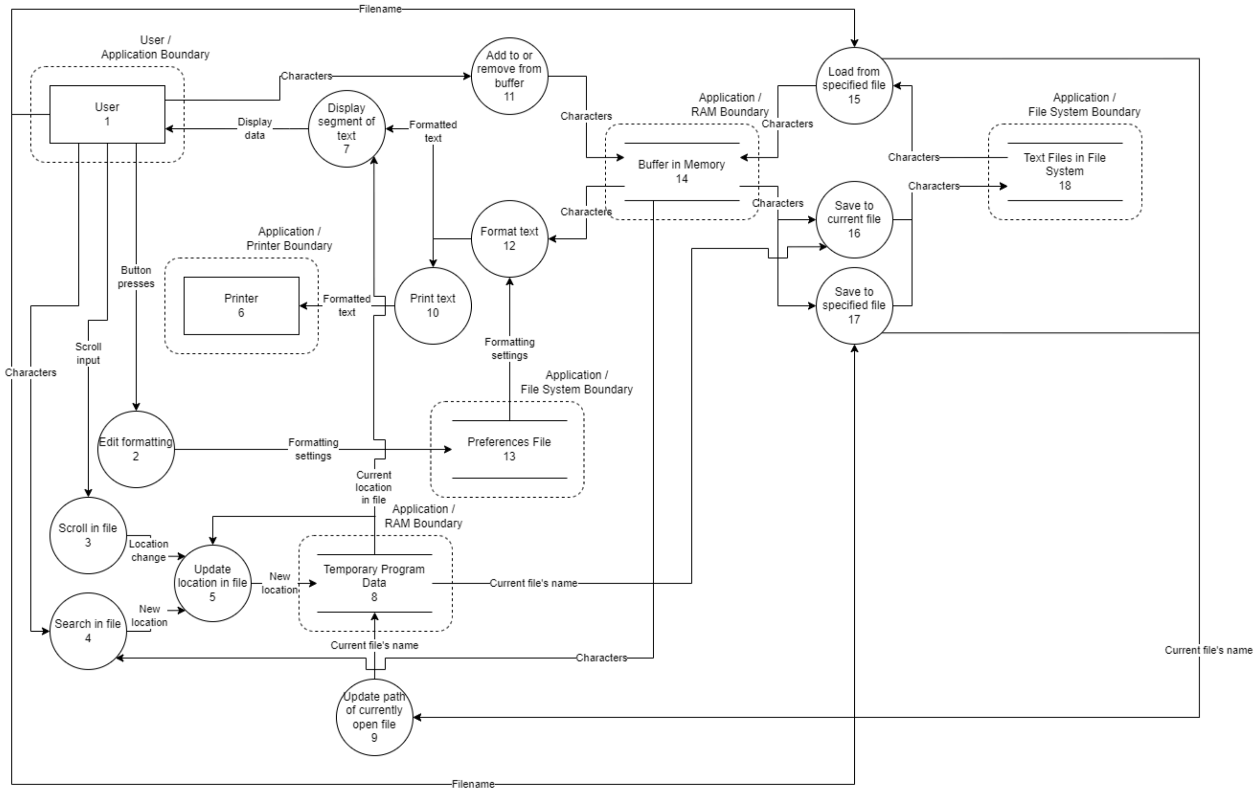
# Table Of Contents

# Description

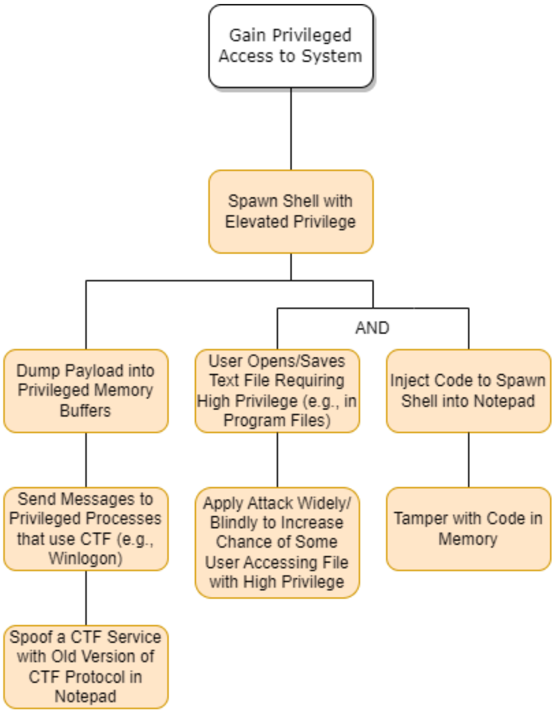
Notepad is a text editor by Microsoft for Windows. Notepad allows users to create, read and write (in a graphical text panel accessing a buffer in memory), and save and load to the device's file system (in a file dialog) plain text files in a specified encoding format. It supports the UTF-8, UTF-16 (big- and little-endian), and ANSI encoding formats.

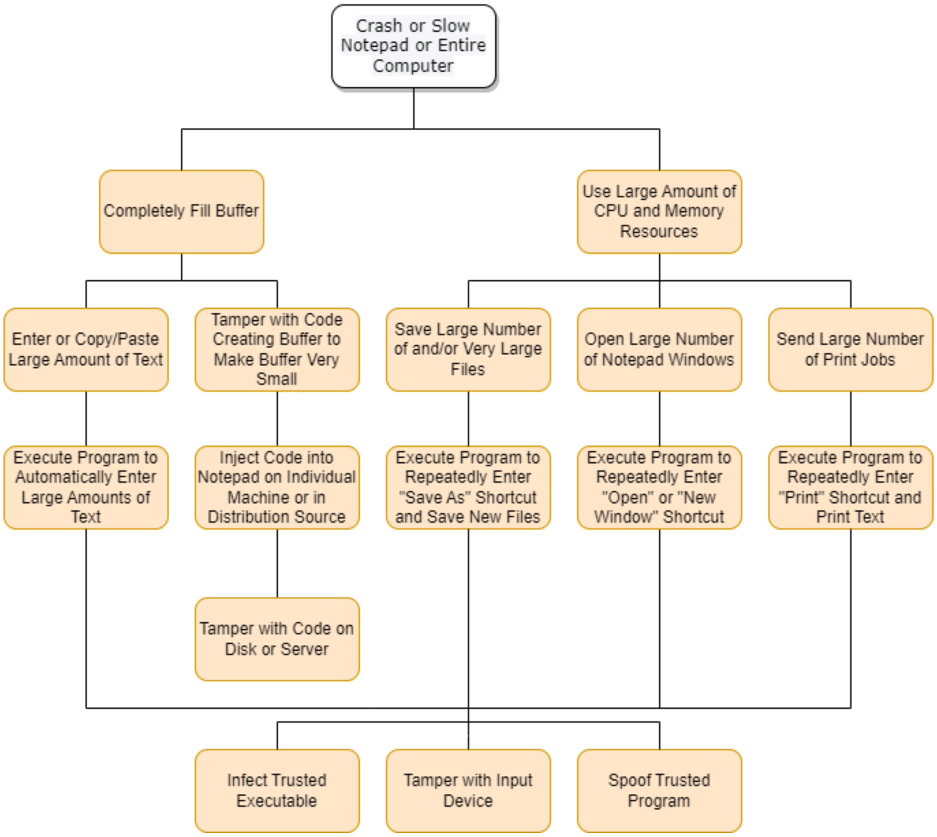
Other features include printing, zooming in and out, searching within a file, searching and replacing within a file, selecting and searching with Bing (in Windows 10), showing a status bar at the bottom of the screen, copying and pasting text, viewing a file with or without word wrapping, and selecting a font, font style (e.g., italic, though options differ between fonts), and font size.

# Data Flow Diagram (DFD)



# Threat Tree


Gain Privileged Access to System
Spawn Shell with Elevated Privilege
AND
Dump Payload into Privileged Memory Buffers
User Opens/Saves Text File Requiring High Privilege (e.g., in Program Files)
Inject Code to Spawn Shell into Notepad
Send Messages to Privileged Processes that use CTF (e.g., Winlogon)
Apply Attack Widely/ Blindly to Increase Chance of Some User Accessing File with High Privilege
Tamper with Code in Memory
Spoof a CTF Service with Old Version of CTF Protocol in Notepad


Crash or Slow Notepad or Entire Computer
Completely Fill Buffer
Use Large Amount of CPU and Memory Resources
Enter or Copy/Paste Large Amount of Text
Tamper with Code Creating Buffer to Make Buffer Very Small
Save Large Number of and/or Very Large Files
Open Large Number of Notepad Windows
Send Large Number of Print Jobs
Execute Program to Automatically Enter Large Amounts of Text
Inject Code into Notepad on Individual Machine or in Distribution Source
Execute Program to Repeatedly Enter "Save As" Shortcut and Save New Files
Execute Program to Repeatedly Enter "Open" or "New Window" Shortcut
Execute Program to Repeatedly Enter "Print" Shortcut and Print Text
Tamper with Code on Disk or Server
Infect Trusted Executable
Tamper with Input Device
Spoof Trusted Program

# STRIDE: Break Down of Threats

Threats are grouped below by the terminators and data stores in the DFD where data crosses the related trust boundary. For each terminator or data store, each threat also provides the number of each connected process from the DFD involved in that threat (e.g., (2), for a threat involving the process numbered 2 in the DFD). If a threat involves multiple categories in STRIDE or multiple terminators or data stores, it is fully described in the earliest category it involves in the earliest terminator or data store, and later categories refer to the threat by the number assigned to it and the category it first appeared in.

Note: Repudiation is excluded because Notepad does not mark user activities as authorized/unauthorized, relying instead on Windows' user accounts and ACLs.

From DFD
1. User (terminator)

- S
    - Threat 1: An attacker is incorrectly authorized by Windows to run Notepad as a certain user, possibly modifying the user's formatting settings in their Preferences File (2) or reading (7, 12, 15) or modifying (11, 16, 17) the user's text files.
        - Mitigation
            - Set passwords on and/or use higher-privilege user accounts for text files containing sensitive information.
- T
    - Threat 1 (in S)
    - Threat 2: An attacker modifies the code for editing the text file (11) or displaying its contents (7, 12) to prevent the user from writing or reading text files as intended.
        - Mitigation
            - Check a digital signature (provided when the program is received from a distribution source) for the program before opening the program to ensure the code was not modified when being downloaded, being installed, or waiting on the disk.
            - Use ASLR to ensure the program's code is not in a predictable location in memory to prevent editing the code in memory.
    - Threat 3: An attacker modifies the code for a process accepting text from the user (11), for input devices, or for a process displaying text to the user (7, 12) to record and transmit the text typed or read by the user in the program.
        - Mitigation

      - Check a digital signature for the program before opening the program to ensure the code has not been modified.
      - Use ASLR to ensure the program's code is not in a predictable location in memory to prevent editing the code in memory.
      - Internally transmit and store the text typed by the user in an encrypted format until it is displayed to increase the number of steps required to successfully perform this attack on some of the surface area vulnerable to it.
- I
  - Threat 1 (in S)
  - Threat 3 (in T)
- D
  - Threat 2 (in T)
  - Threat 4: An attacker causes a large number of windows of the application to open, using CPU and memory resources to slow or crash the program or the user's device.
    - Mitigation
      - Limit the number of windows of the application that can be open at the same time.
      - Limit the amount of CPU and memory resources that can be devoted to the entire application.
      - Require a slight delay after opening a new window before another new window can be opened, slowing down such an attack.
- E
  - None
    - No additional privilege is directly required for any operations of the user interface.

6. Printer (terminator)
- S
  - Threat 5: A process or device impersonates a trusted printer connected to the user's computer to reroute the printed text output (10) to an attacker.
    - Mitigation
      - Require the printer to provide a secret key to the user's device to validate the printer before the file is sent.
      - Use asymmetric cryptography with a public key sent by the printer for the user's device to encrypt the file with (or symmetric cryptography with the key transmitted using asymmetric cryptography, if asymmetric cryptography is too slow for the files to be printed).
- T

  - Threat 6: An attacker modifies the code for reading (12) or printing (10) a text file to transmit the text to the attacker or prevent the user from successfully printing their file.
    - Mitigation
      - Check a digital signature for the program before opening the program to ensure the code has not been modified.
      - Use ASLR to ensure the program’s code is not in a predictable location in memory to prevent editing the code in memory.
      - Transmit and store the text in an encrypted format to increase the steps required to succeed in such an attack.
  - Threat 7: An attacker modifies the code for printing (10) a text file to allow other print jobs to be sent while the privileges or resources required for sending a print job are held by the code for printing the text file, potentially printing many other pages and preventing the printer from being used as intended.
    - Mitigation
      - Check a digital signature for the program before opening the program to ensure the code has not been modified.
      - Use ASLR to ensure the program’s code is not in a predictable location in memory to prevent editing the code in memory.
      - Ensure that any needed privileges are acquired only as soon as they need to be used and are dropped as soon as possible to limit the span of code and time in which an attack could be successful.
- I
  - Threat 5 (in S)
  - Threat 6 (in T)
- D
  - Threat 6 (in T)
  - Threat 7 (in T)
- E
  - Threat 7 (in T)

8. Temporary Program Data (data store)
   - S
     - None
       - The user’s location in a file and the path of the current file are only stored for the current session of the program, so impersonating a user to run the program does not risk this data (although means other than impersonation can be used to take control of a session being currently run by a valid user).
   - T

- Threat 8: An attacker modifies a process writing to memory (5, 11, 15) to incorrectly write another section of memory, crashing the program or affecting other programs or data.
    - Mitigation
        - Check a digital signature for the program before opening the program to ensure the code has not been modified.
        - Use ASLR to ensure the program's code is not in a predictable location in memory to prevent editing the code in memory.
        - Check that the memory addresses used in the processes are within a valid range for the allocated memory they should write to before attempting to write to memory.
- Threat 9: An attacker modifies a process reading from (5, 12, 16, 17) or writing to (5, 9, 11, 15) memory to prevent the user from reading or writing text files as intended.
    - Mitigation
        - Check a digital signature for the program before opening the program to ensure the code has not been modified.
        - Use ASLR to ensure the program's code is not in a predictable location in memory to prevent editing the code in memory.
- Threat 10: An attacker modifies a process writing to memory (5, 9, 11, 15) to use the application's access privileges for the application's own memory to make arbitrary modifications to the memory allocated to the program, sidestepping Windows' program-specific memory protections and potentially acquiring higher privilege by then modifying code in the program that uses other privileges.
    - Mitigation
        - Check a digital signature for the program before opening the program to ensure the code has not been modified.
        - Use ASLR to ensure the program's code is not in a predictable location in memory to prevent editing the code in memory.
        - Divide the program into formal subprograms to make program-specific memory protections more granular, limiting the scope of such a tampering attack.
- Threat 11: An attacker modifies the code for updating the user's location in the file (3, 4, 5) or for updating the current file path (9) to prevent the program from displaying or saving the file correctly.
    - Mitigation
        - Check a digital signature for the program before opening the program to ensure the code has not been modified.
        - Use ASLR to ensure the program's code is not in a predictable location in memory to prevent editing the code in memory.

                - Include different, secondary processes for each of these operations to be used in the event of a detected failure of the primary processes.
        - Threat 12: An attacker finds program data in memory and changes the path stored for which file is currently open, causing the text to be saved (16, 17) to somewhere the attacker can more easily access.
            - Mitigation
                - Use ASLR (if the memory used is statically allocated) to ensure the program's code is not in a predictable location in memory, or dynamically allocate the required memory to have the OS provide a less predictable location in memory.
                - Store the temporary program data in an encoded format to make precisely editing it more difficult.
    - I
        - Threat 12 (in T)
        - Threat 13: An attacker finds the program data in memory and reads the path of the currently open file, gaining information about a file and several folders on the user's device.
            - Mitigation
                - Use ASLR (if the memory used is statically allocated) to ensure the program's code is not in a predictable location in memory, or dynamically allocate the required memory to have the OS provide a less predictable location in memory.
                - Store the temporary program data in an encoded format to make any discovered data less likely to be usable.
    - D
        - Threat 8 (in T)
        - Threat 9 (in T)
        - Threat 11 (in T)
    - E
        - Threat 10 (in T)

13. Preferences File (data store)
    - S
        - Only through user spoofing — Threat 1 (in 1.S)
    - T
        - Threat 2 (in 1.T) - with invalid/no formatting information
        - Threat 14: An attacker modifies the formatting information in the persistent preferences file to make text files difficult for the user to read (7, 12) or crash the program.
            - Mitigation

      - Use ACL or a secret key held by the program to make editing the preferences file outside of the program more difficult.
      - If invalid formatting information is provided from the file, either fail securely and close or revert to default formatting settings specified in the code.
      - Generate a digital signature for the preferences file when closing the program, store the signature securely, and check the digital signature before loading the preferences into memory when opening the program to ensure that the preferences file has not been modified externally.
  - Threat 15: An attacker modifies or causes unexpected behavior in a process reading from (12, 15) or writing to (2, 16, 17) the file system while that process holds read or write privileges, allowing the attacker to execute code with those privileges (potentially even high-level read and write privileges if the user is viewing or editing text files in a directory where such privileges are required — such as Program Files).
    - Mitigation
      - Use ACLs on all files to require only the minimum amount of privilege needed to use them as intended.
      - Ensure that needed privileges within a process are acquired only as soon as they are required, are dropped as soon as they are no longer required, and are always dropped even in the event of a failure within the process.
      - Avoid saving and reading text files in high-privilege folders when not dealing with sensitive information in order to avoid unnecessarily acquiring higher privileges for any length of time.
- I
  - None
    - Preferred font and font size are very likely not sensitive information (although more serious information disclosure may occur through elevation of privilege from Threat 15).
- D
  - Threat 2 (in 1.T)
  - Threat 14 (in T)
- E
  - Threat 15 (in T)

14. Buffer in Memory (data store)
   - S
     - Only through user spoofing — Threat 1 (in 1.S)
   - T

  - Threat 8 (in 8.T)
  - Threat 9 (in 8.T)
  - Threat 10 (in 8.T)
  - Threat 16: An attacker modifies a process reading from the character buffer (12) to incorrectly read another section of memory and display it to the user (7) in the expected text encoding.
    - Mitigation
      - Check a digital signature for the program before opening the program to ensure the code has not been modified.
      - Use ASLR to ensure the program's code is not in a predictable location in memory to prevent editing the code in memory.
      - Check that the memory addresses used in the process are within a valid range for the allocated memory they should read from before attempting to read from memory.
  - Threat 17: An attacker modifies character data in the buffer to make the file unreadable or unusable, possibly also propagating those changes to the version of the file on the file system if saved (16, 17) after being modified.
    - Mitigation
      - Use ASLR (if the buffer is statically allocated) to ensure the buffer is not in a predictable location in memory, or dynamically allocate the buffer to have the OS provide a less predictable location in memory.
  - Threat 18: An attacker modifies the code allocating the buffer to shrink the buffer size, allowing the buffer to more quickly completely fill and slow or crash the program.
    - Mitigation
      - Check a digital signature for the program before opening the program to ensure the code was not modified.
      - Use ASLR to ensure the program's code is not in a predictable location in memory.
      - Allow the buffer to expand dynamically to a certain point.
      - Check whether the buffer is full before writing to it and otherwise ensure that no data is written outside of the buffer.
      - Do not cause the program to forcibly close when the buffer is full, or (if the program must close in this event for some reason) ensure that all resources are closed and all privileges are dropped before closing the program.
- I
  - Threat 16 (in T)

  - Threat 19: An attacker finds the character buffer in memory and reads the contents of the user’s text file.
    - Mitigation
      - Use ASLR (if the buffer is statically allocated) to ensure the buffer is not in a predictable location in memory, or dynamically allocate the buffer to have the OS provide a less predictable location in memory.
      - Store the character data in an encoded format to make precisely editing it more difficult.
- D
  - Threat 8 (in 8.T)
  - Threat 9 (in 8.T)
  - Threat 17 (in T)
  - Threat 20: An attacker causes a large amount of text to be sent to the buffer, making the buffer fill to the extent that the program or device slows or crashes.
    - Mitigation
      - Limit the amount of data that can be pasted into the text area at once.
      - Check whether the buffer is full before writing to it and otherwise ensure that no data is written outside of the buffer.
      - Do not cause the program to forcibly close when the buffer is full, or (if the program must close in this event for some reason) ensure that all resources are closed and all privileges are dropped before closing the program.
- E
  - Threat 10 (in 8.T)

18. Text Files in File System (data store)
    - S
      - Threat 1 (in 1.S)
      - Threat 21: An attacker creates a very large file with a similar name to one of the user’s files or an otherwise believable name for a text file, consuming CPU and RAM resources and causing the program or device to slow or crash when opening (15), processing (12), or displaying the file (7).
        - Mitigation
          - Prompt the user to confirm opening very large files before attempting to load or display them, allowing the user to cancel potentially dangerous operations.
          - Before opening a file created or modified by another author, display the provided author name and prompt the user to confirm that they wish to open the file.

      - Limit the maximum size of files that can be loaded into the application.
- T
  - Threat 9 (in 8.T)
  - Threat 15 (in 13.T)
  - Threat 22: An attacker modifies text files incorrectly through some other application and makes the text files unreadable (12, 15) for Notepad.
    - Mitigation
      - Use passwords and/or ACLs for higher-privilege user accounts to secure text files containing information that must be carefully preserved.
      - Keep backups of text files and allow the user to rollback to previous versions of their text files. This feature should have an option to be disabled for sensitive files that the user wants to manually keep track of all copies of.
  - Threat 23: An attacker modifies the processes for saving (16, 17) or loading (15) a file or for managing the user interface to open a file dialog to retrieve information about the folders and files on the user's device.
    - Mitigation
      - Check a digital signature for the program before opening the program to ensure the code was not modified.
      - Use ASLR to ensure the program's code is not in a predictable location in memory.
      - Ensure that the privileges required for opening a file dialog are acquired only as soon as they are needed and are dropped as soon as they are no longer needed.
  - Threat 24: An attacker modifies the processes for saving files (16, 17) or requesting that files be saved from the user interface in order to store a large number of and/or very large files, slowing or crashing the program or device.
    - Mitigation
      - Check a digital signature for the program before opening the program to ensure the code was not modified.
      - Use ASLR to ensure the program's code is not in a predictable location in memory.
      - Ensure that the privileges needed for saving the file are acquired only as soon as they are needed and are dropped as soon as they are no longer needed.
      - Limit the amount of times the application can save a file within a certain time frame.

- Limit the amount of resources the application can use at one time for saving files, slowing down such attacks and reducing their effectiveness for using any resources other than disk space.

- I
  - Threat 15 (in 13.T)
  - Threat 23 (in T)
- D
  - Threat 9 (in 8.T)
  - Threat 21 (in T)
  - Threat 22 (in T)
  - Threat 24 (in T)
- E
  - Threat 15 (in 13.T)

Other

- E
  - Threat 25: An attacker utilizes vulnerabilities in old versions of the CTF protocol (used for translating text provided to the program) when sending messages between windows to spawn a shell with system-level privileges.
    - Mitigation
      - Validate that all messages sent by other windows come from processes with the required privileges for the requests they make.
      - Ignore any requests other windows send that are not explicitly part of the required functionality of the application.
      - Keep local copies of the program up-to-date with security patches as soon as such bugs are known.
    - Reported at https://googleprojectzero.blogspot.com/2019/08/down-rabbit-hole.html

# DREAD: Ranking of Threats

Table of Threats and Ratings Sorted by Total:

| Threat | D | R | E | A | D | Total | Rating |
|---|---|---|---|---|---|---|---|
| 25 | 10 | 6 | 5 | 3 | 10 | 6.8 | Medium |
| 5 | 5 | 4 | 8 | 5 | 8 | 6 | Medium |
| 15 | 10 | 8 | 2 | 2 | 4 | 5.2 | Medium |
| 10 | 10 | 7 | 2 | 2 | 4 | 5 | Medium |
| 21 | 5 | 7 | 5 | 2 | 6 | 5 | Medium |
| 7 | 6 | 6 | 2 | 5 | 4 | 4.6 | Medium |
| 22 | 5 | 7 | 4 | 2 | 5 | 4.6 | Medium |
| 8 | 6 | 6 | 2 | 2 | 4 | 4 | Low |
| 1 | 6 | 6 | 2 | 2 | 3 | 3.8 | Low |
| 3 | 5 | 6 | 2 | 2 | 4 | 3.8 | Low |
| 4 | 6 | 4 | 3 | 2 | 4 | 3.8 | Low |
| 20 | 2 | 4 | 5 | 2 | 6 | 3.8 | Low |
| 16 | 6 | 4 | 2 | 2 | 4 | 3.6 | Low |
| 23 | 6 | 5 | 1 | 2 | 4 | 3.6 | Low |
| 24 | 6 | 3 | 2 | 2 | 4 | 3.4 | Low |
| 6 | 2 | 6 | 2 | 2 | 4 | 3.2 | Low |
| 19 | 5 | 4 | 2 | 2 | 3 | 3.2 | Low |
| 2 | 1 | 6 | 2 | 2 | 4 | 3 | Low |
| 9 | 1 | 6 | 2 | 2 | 4 | 3 | Low |
| 13 | 4 | 4 | 2 | 2 | 3 | 3 | Low |
| 14 | 2 | 6 | 2 | 2 | 3 | 3 | Low |
| 17 | 5 | 4 | 1 | 2 | 3 | 3 | Low |

| Threat | D | R | E | A | D | Total | Rating |
|---|---|---|---|---|---|---|---|
| 18 | 2 | 6 | 1 | 2 | 4 | 3 | Low |
| 11 | 1 | 6 | 2 | 2 | 3 | 2.8 | Low |
| 12 | 5 | 3 | 1 | 2 | 3 | 2.8 | Low |

Threat 1: An attacker is incorrectly authorized by Windows to run Notepad as a certain user, possibly modifying the user's formatting settings in their Preferences File (2) or reading (7, 12, 15) or modifying (11, 16, 17) the user's text files.

- D: 6
    - May cause leakage or modification of sensitive information in user files
- R: 6
    - Is simple to reproduce if account details or a vulnerability in Windows are found (in which case, Notepad likely is not the focus)
- E: 2
    - Requires acquiring a user's account credentials or finding and exploiting a vulnerability in well-tested code or in Windows' user-authentication system
- A: 2
    - Affects an individual user or possibly a single system
- D: 3
    - Requires discovering another digital or social vulnerability but uses common parts of the application

Overall threat rating: 3.8

Threat 2: An attacker modifies the code for editing the text file (11) or displaying its contents (7, 12) to prevent the user from writing or reading text files as intended.

- D: 1
    - Makes reading or writing text files in Notepad difficult
- R: 6
    - Reliably causes difficulties for the user if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3

Threat 3: An attacker modifies the code for a process accepting text from the user (11), for input devices, or for a process displaying text to the user (7, 12) to record and transmit the text typed or read by the user in the program.

- D: 5
    - May cause leakage of sensitive information typed or read by the user in the program
- R: 6
    - Reliably affects the user if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3.8

Threat 4: An attacker causes a large number of windows of the application to open, using CPU and memory resources to slow or crash the program or the user's device.

- D: 6
    - May slow down or crash the program or system, causing difficulties and possibly leading to other threats
- R: 4
    - Somewhat reliably affects users if resource limits do not strongly affect the program
- E: 3
    - Requires launching an application on the user's machine or sending signals to a running instance of the program to open new windows
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3.8

Threat 5: A process or device impersonates a trusted printer connected to the user's computer to reroute the printed text output (10) to an attacker.

- D: 5
    - May cause leakage of sensitive information from text files printed by the user and prevent intended printing
- R: 4
    - Can be reliably reproduced within a window of time when the user will attempt to print
- E: 8
    - Requires simple spoofing of a name, IP, and/or other information associated with a printer and requires a connection to a network the user is connected to
- A: 5
    - May affect several users and devices attempting to connect to the printer
- D: 8
    - Is widely known and publicly explained

Overall threat rating: 6

Threat 6: An attacker modifies the code for reading (12) or printing (10) a text file to transmit the text to the attacker or prevent the user from successfully printing their file.

- D: 2
    - May cause leakage of sensitive information typed or printed by the user in the program
- R: 6
    - Reliably affects the user if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3.2

Threat 7: An attacker modifies the code for printing (10) a text file to allow other print jobs to be sent while the privileges or resources required for sending a print job are held by the code for printing the text file, potentially printing many other pages and preventing the printer from being used as intended.

- D: 6
    - May allow wasteful external use of a local physical device and prevent intended printing
- R: 6

    - Reliably affects the user if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 5
    - May affect several users and devices relying on the printer
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 4.6

Threat 8: An attacker modifies a process writing to memory (5, 11, 15) to incorrectly write another section of memory, crashing the program or affecting other programs or data.

- D: 6
    - May prevent the user from using the program or other programs and possibly cause other threats through crashes
- R: 6
    - Reliably affects the user if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 4

Threat 9: An attacker modifies a process reading from (5, 12, 16, 17) or writing to (5, 9, 11, 15) memory to prevent the user from reading or writing text files as intended.

- D: 1
    - Prevents reading or writing text files in Notepad
- R: 6
    - Reliably affects the user if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4

    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3

Threat 10: An attacker modifies a process writing to memory (5, 9, 11, 15) to use the application's access privileges for the application's own memory to make arbitrary modifications to the memory allocated to the program, sidestepping Windows' program-specific memory protections and potentially acquiring higher privilege by then modifying code in the program that uses other privileges.

- D: 10
    - Provides elevated privilege
- R: 7
    - Reliably allows attacker to perform further attacks if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 5

Threat 11: An attacker modifies the code for updating the user's location in the file (3, 4, 5) or for updating the current file path (9) to prevent the program from displaying or saving the file correctly.

- D: 1
    - Makes reading or writing text files in Notepad difficult
- R: 6
    - Reliably causes difficulties for the user if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 3
    - Requires discovering another vulnerability but attacks somewhat common parts of the application

Overall threat rating: 2.8

Threat 12: An attacker finds program data in memory and changes the path stored for which file is currently open, causing the text to be saved (16, 17) to somewhere the attacker can more easily access.

- D: 5
    - May cause leakage of sensitive information typed or read by the user in the program
- R: 3
    - Requires correct timing to ensure the user saves the file after the path has been changed
- E: 1
    - Requires modifying the application's data in memory by means not provided by the program and requires the attacker to have a location on the disk they can easily read data from
- A: 2
    - Affects an individual user or possibly a single system
- D: 3
    - Requires discovering another vulnerability but attacks somewhat common parts of the application

Overall threat rating: 2.8

Threat 13: An attacker finds the program data in memory and reads the path of the currently open file, gaining information about a file and several folders on the user's device.

- D: 4
    - May leak sensitive information about some of the folders and files on the user's device
- R: 4
    - Reliably retrieves information if the application is running and the relevant memory is found
- E: 2
    - Requires finding the application's data in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 3
    - Requires discovering another vulnerability but attacks somewhat common parts of the application

Overall threat rating: 3

Threat 14: An attacker modifies the formatting information in the persistent preferences file to make text files difficult for the user to read (7, 12) or crash the program.

- D: 2
  - Makes reading or writing text files in Notepad difficult and possibly crashes the program
- R: 6
  - Reliably causes difficulties for the user if the application is successfully tampered with
- E: 2
  - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
  - Affects an individual user or possibly a single system
- D: 3
  - Requires discovering another vulnerability but attacks somewhat common parts of the application

Overall threat rating: 3

Threat 15: An attacker modifies or causes unexpected behavior in a process reading from (12, 15) or writing to (2, 16, 17) the file system while that process holds read or write privileges, allowing the attacker to execute code with those privileges (potentially even high-level read and write privileges if the user is viewing or editing text files in a directory where such privileges are required — such as Program Files).

- D: 10
  - May leak information and provide elevated privileges
- R: 8
  - Reliably allows attacker to perform further attacks if the application is successfully tampered with or if unexpected behavior is caused in certain processes
- E: 2
  - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
  - Affects an individual user or possibly a single system
- D: 4
  - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 5.2

Threat 16: An attacker modifies a process reading from memory (12) to incorrectly read another section of memory and display it to the user (7) in the expected text encoding.

- D: 6
    - May display sensitive information from memory in a difficult-to-read format in the text panel
- R: 4
    - May reliably retrieve some unintended information from memory if the application is successfully tampered with
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3.6

Threat 17: An attacker modifies or corrupts character data in the buffer to make the file unreadable and possibly propagate those changes to the version of the file on the file system if saved (16, 17) after being modified.

- D: 5
    - May prevent the user from reading or writing files with Notepad and destroy data in some files
- R: 4
    - Reliably affects the user if the application's data in memory is successfully tampered with but requires correct timing to affect the user's files
- E: 1
    - Requires finding and modifying the application's data in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 3
    - Requires discovering another vulnerability but attacks somewhat common parts of the application

Overall threat rating: 3

Threat 18: An attacker modifies the code allocating the buffer to shrink the buffer size, allowing the buffer to more quickly completely fill and slow or crash the program.

- D: 2

    - Makes reading or writing text files in Notepad difficult and possibly crashes the program
- R: 6
    - Reliably affects the user if the application is successfully tampered with
- E: 1
    - Requires modifying the application in program files or finding and modifying the application in memory and may require additional knowledge of the program's code
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3

Threat 19: An attacker finds the character buffer in memory and reads the contents of the user's text file.

- D: 5
    - May cause leakage of sensitive information typed or read by the user in the program
- R: 4
    - Reliably retrieves information if the application is running and the relevant memory is found
- E: 2
    - Requires finding the application's data in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 3
    - Requires discovering another vulnerability but attacks somewhat common parts of the application

Overall threat rating: 3.2

Threat 20: An attacker causes a large amount of text to be sent to the buffer, making the buffer fill to the extent that the program or device slows or crashes.

- D: 2
    - Makes reading or writing text files in Notepad difficult and possibly crashes the program
- R: 4
    - Somewhat reliably affects users if resource limits do not strongly affect the program

- E: 5
    - Requires sending typing or copy/paste input to the user’s machine from some program or input device
- A: 2
    - Affects an individual user or possibly a single system
- D: 6
    - Uses a common part of the program

Overall threat rating: 3.8

Threat 21: An attacker creates a very large file with a similar name to one of the user’s files or an otherwise believable name for a text file, consuming CPU and RAM resources and causing the program or device to slow or crash when opening (15), processing (12), or displaying the file (7).

- D: 5
    - May slow down the program or device and cause a crash
- R: 7
    - Reliably affects the user if they open the file
- E: 5
    - Requires creating a large text file and placing on the user’s device
- A: 2
    - Affects an individual user or possibly a single system
- D: 6
    - Uses a common part of the program

Overall threat rating: 5

Threat 22: An attacker modifies text files incorrectly through some other application and makes the text files unreadable (12, 15) for Notepad.

- D: 5
    - May prevent the user from reading or writing files with Notepad and destroy data in some files
- R: 7
    - Reliably affects the user if a text file they use is modified
- E: 4
    - Requires modifying a text file on the user’s device
- A: 2
    - Affects an individual user or possibly a single system
- D: 5
    - Requires discovering another vulnerability but clearly affects the user in a direct way

Overall threat rating: 4.6

Threat 23: An attacker modifies the processes for saving (16, 17) or loading (15) a file or for managing the user interface to open a file dialog to retrieve information about the folders and files on the user's device.

- D: 6
    - May leak sensitive information about many folders and files on the user's device
- R: 5
    - Reliably retrieves information if the application is successfully tampered with and if the file dialog can be reliably viewed in some form by the attacker
- E: 1
    - Requires modifying the application in program files or finding and modifying the application in memory and requires a way to view the resulting file dialog
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3.6

Threat 24: An attacker modifies the processes for saving files (16, 17) or requesting that files be saved from the user interface in order to store a large number of and/or very large files, slowing or crashing the program or device.

- D: 6
    - May slow down or crash the program or system, causing difficulties and possibly leading to other threats
- R: 3
    - Reliably affects the user if the application is successfully tampered with and if resource limits do not strongly affect the program
- E: 2
    - Requires modifying the application in program files or finding and modifying the application in memory
- A: 2
    - Affects an individual user or possibly a single system
- D: 4
    - Requires discovering another vulnerability but attacks common parts of the application

Overall threat rating: 3.4

Threat 25: An attacker utilizes vulnerabilities in old versions of the CTF protocol (used for translating text provided to the program) when sending messages between windows to spawn a shell with system-level privileges.

- D: 10
  - Provides system-level privileges
- R: 6
  - Reliably allows attacker to perform further attacks if the user’s version of the application uses an old version of the CTF protocol
- E: 5
  - Requires some tools, technical knowledge, and a connection the user’s device but is not possible on patched versions accounting for the old protocol
- A: 3
  - Affects at least one system
- D: 10
  - Is widely known, is publicly explained, and has widely available tools for performing the attack

Overall threat rating: 6.8