File Audit Report

September 21st, 2025

[redacted]

[redacted]

Jessica [redacted]

Yuri [redacted]

Elke [redacted]

Safa [redacted]

Matthew [redacted]

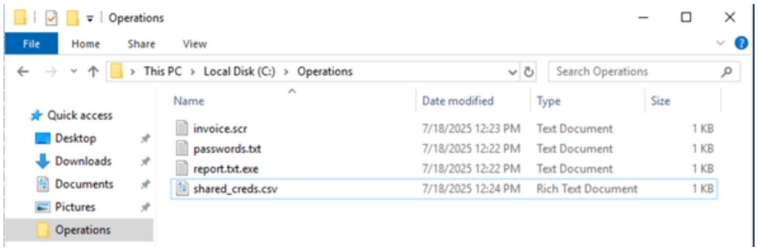
Executive Summary

[redacted] was granted access to a Windows 2019 Server for a file audit. During the assessment, several critical vulnerabilities were discovered:

- Unencrypted plaintext credentials.
- Files disguised as unencrypted plaintext credentials that may contain malware.
- Exposed account references to both the privileged and guest users.

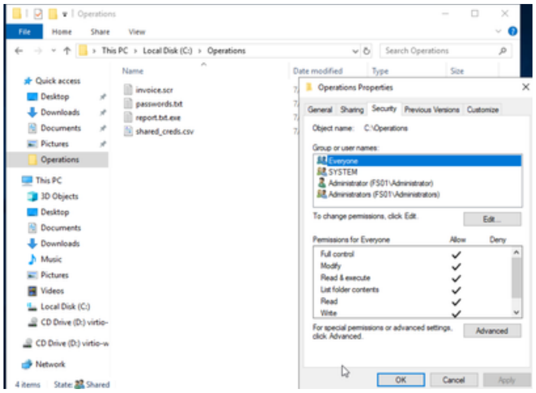
These critical vulnerabilities increase the risk of data leakage, unauthorized access, and a fully compromised system. Immediate remediation is recommended for the protection of the system's essential assets.

Screenshot 1: A critical vulnerability of unprotected sensitive file exposure. A folder with plain text files which indicates exactly what is stored inside (e.g. passwords.txt).



Name	Date modified	Type	Size
invoice.scr	7/18/2025 12:23 PM	Text Document	1 KB
passwords.txt	7/18/2025 12:22 PM	Text Document	1 KB
report.txt.exe	7/18/2025 12:22 PM	Text Document	1 KB
shared_creds.csv	7/18/2025 12:24 PM	Rich Text Document	1 KB

Screenshot 2: Another critical vulnerability of overly permissive permissions. Every user has access with all permissions enabled.



Operations Properties

Object name: C:\Operations

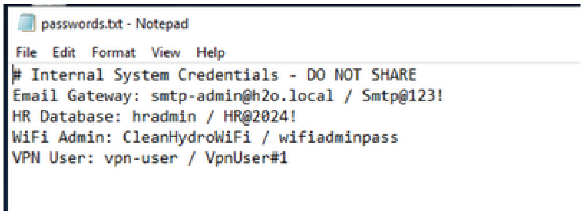
Group or user names:
Everyone
SYSTEM
Administrator (FS01\Administrator)
Administrators (FS01\Administrators)

To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

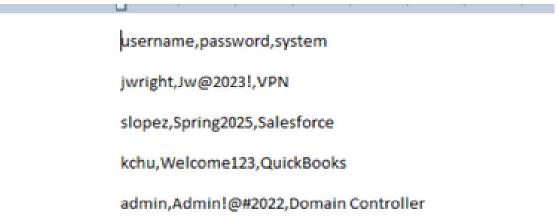
Screenshot 3: Additional critical vulnerability of improper storage of sensitive information. Internal system credentials are stored in an unencrypted plaintext file.



```
# Internal System Credentials - DO NOT SHARE
Email Gateway: smtp-admin@h2o.local / Smtp@123!
HR Database: hradmin / HR@2024!
WiFi Admin: CleanHydroWiFi / wifiadminpass
VPN User: vpn-user / VpnUser#1
```

Appendix

Screenshot 4 - 6: Additional examples of the critical vulnerability of improper storage of sensitive information, all in unencrypted, plain text files.



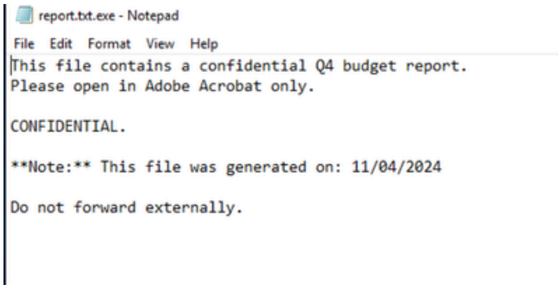
```
username,password,system

jwright,Jw@2023!,VPN

slopez,Spring2025,Salesforce

kchu,Welcome123,QuickBooks

admin,Admin!@#2022,Domain Controller
```

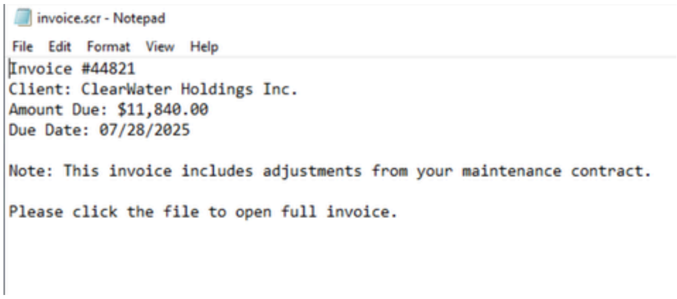


```
This file contains a confidential Q4 budget report.
Please open in Adobe Acrobat only.

CONFIDENTIAL.

**Note:** This file was generated on: 11/04/2024

Do not forward externally.
```



```
Invoice #44821
Client: ClearWater Holdings Inc.
Amount Due: $11,840.00
Due Date: 07/28/2025

Note: This invoice includes adjustments from your maintenance contract.

Please click the file to open full invoice.
```

Mitigation Steps

For the best security practices, this server is recommended to follow a formed security plan in order to mitigate their vulnerabilities:

1. Immediate removal of malicious files in order to avoid:
   a. Causing general damage to the system.
   b. Data harvesting and exfiltration.
   c. Potential financial loss.
2. Changing vulnerable credentials to prevent unauthorized access.
3. Implementation of least-privilege access controls to minimize any internal misuse of the system.
4. Encryption of sensitive data to protect against data leaks.
5. Enabling monitoring/logging for future anomalies.