

**Security Assessment Findings Report**

HF-SRV-DATACOLOR – 10.40.62.18

A logo for a company

Description automatically generated

Confidential

Table of Contents

[Confidentiality Statement 3](#_Toc184384503)

[Disclaimer 3](#_Toc184384504)

[Assessment Overview 3](#_Toc184384505)

[Finding Severity Ratings 4](#_Toc184384506)

[Scope 4](#_Toc184384507)

[Vulnerability Summary 1](#_Toc184384508)

[Technical Findings 2](#_Toc184384509)

[Critical Vulnerabilities 2](#_Toc184384510)

[Windows Server 2016 Security Update (November 2024) 2](#_Toc184384511)

[High Vulnerabilities 3](#_Toc184384512)

[Security Updates for Microsoft .NET Framework (October 2024) 3](#_Toc184384513)

[VMware Tools Vulnerabilities. 3](#_Toc184384514)

[WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck) 4](#_Toc184384515)

[Medium Vulnerabilities 5](#_Toc184384516)

[SSL Medium Strength Cipher Suites Supported (SWEET32) 5](#_Toc184384517)

[TLS Version 1.0 Protocol Detection 5](#_Toc184384518)

[TLS Version 1.1 Deprecated Protocol 6](#_Toc184384519)

[SMB Signing not required 6](#_Toc184384520)

[Additional Scans and Reports 7](#_Toc184384521)

# Confidentiality Statement

This document is the exclusive property of Hayleys Fabric and Fentons IT (FIT) and contains proprietary and confidential information. Any duplication, redistribution, or use, in whole or in part, in any format, is strictly prohibited without prior consent from both Hayleys Fabric and FIT. Hayleys Fabric reserves the right to share this document with auditors under non-disclosure agreements to meet compliance requirements.

# Disclaimer

A Vulnerability Assessment represents a specific point in time, with its findings and recommendations based on the information collected during the assessment period. It does not account for any changes or modifications made afterward. FIT focused the assessment on identifying the weakest security controls that attackers might exploit. To maintain the effectiveness of security controls, FIT recommends conducting similar assessments annually.

# Assessment Overview

From December 2, 2024, to December 5, 2024, Hayleys Fabric collaborated with FIT to assess the security posture of its infrastructure in alignment with current industry best practices. This evaluation included an internal network Vulnerability Assessment. The testing was conducted following the guidelines of the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, complemented by customized testing frameworks.

* Planning – Customer goals are gathered and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Reporting – Document all found vulnerabilities and exploits and actionable recommendations to improve the security posture.

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS V3**  **Score Range** | **Definition** |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Scope

|  |  |
| --- | --- |
| **Assessment Type** | Infrastructure Vulnerability Assessment |
| **Asset Name** | HF-SRV-DATACOLOR – 10.40.62.18 |
| **Date** | 02/12/2024 |
| **Conducted By** | Cyber Security Unit Fentons IT |
| **Tools Used** | Nessus, SecPoint |

# Vulnerability Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 3 | 4 | 0 | 20 |
| **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** | **INFO** |

|  |  |
| --- | --- |
| **Finding** | **Severity** |
| Windows Server 2016 Security Update (November 2024) | Critical |
| Security Updates for Microsoft .NET Framework (October 2024) | High |
| VMware Tools Vulnerabilities. | High |
| WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck) | High |
| SSL Medium Strength Cipher Suites Supported (SWEET32) | Medium |
| TLS Version 1.0 Protocol Detection | Medium |
| TLS Version 1.1 Deprecated Protocol | Medium |
| SMB Signing not required | Medium |

# Technical Findings

# Critical Vulnerabilities

## Windows Server 2016 Security Update (November 2024)

|  |  |
| --- | --- |
| **Criticality** | **Critical** |
| **Synopsis** | The remote Windows host is affected by multiple missing patches. |
| **Description** | Windows host is missing security update **5046612**. It is, therefore, affected by multiple vulnerabilities   *- Windows Kerberos Remote Code Execution Vulnerability (CVE-2024-43639)  - Windows NT OS Kernel Elevation of Privilege Vulnerability (CVE-2024-43623)  - Windows Telephony Service Elevation of Privilege Vulnerability (CVE-2024-43626)*  Windows host is missing security update **5044293**. It is, therefore, affected by multiple vulnerabilities  - *Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability (CVE-2024-38212, CVE-2024-38261, CVE-2024-38265, CVE-2024-43453, CVE-2024-43549, CVE-2024-43564, CVE-2024-43589, CVE-2024-43592, CVE-2024-43593, CVE-2024-43607, CVE-2024-43608, CVE-2024-43611)  - Windows Netlogon Elevation of Privilege Vulnerability (CVE-2024-38124)  - Remote Desktop Client Remote Code Execution Vulnerability (CVE-2024-43599)*  Windows host is missing security update **5043051**. It is, therefore, affected by multiple vulnerabilities   *- Windows MSHTML Platform Spoofing Vulnerability (CVE-2024-43461)  - Windows Remote Desktop Licensing Service Spoofing Vulnerability (CVE-2024-43455)  - Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability (CVE-2024-38260, CVE-2024-38263, CVE-2024-43454, CVE-2024-43467)* |
| **Recommendation** | Apply Security Update 5046612/5044293/5043051 |
| **Evidence** | C:\Windows\system32\ntoskrnl.exe has not been patched.  Remote version : 10.0.14393.7254  Should be : 10.0.14393.7513 |

# High Vulnerabilities

## Security Updates for Microsoft .NET Framework (October 2024)

|  |  |
| --- | --- |
| **Criticality** | **High** |
| **Synopsis** | The Microsoft .NET Framework installation on the remote host is missing a security update. |
| **Description** | The Microsoft .NET Framework installation on the remote host is missing a security update. It is, therefore, affected by multiple denial of service vulnerabilities, as follows:   *- A denial of service (DoS) vulnerability. An attacker can exploit this issue to cause the affected component to deny system or application services. (CVE-2024-43483, CVE-2024-43484)* |
| **Recommendation** | Microsoft has released security updates for Microsoft .NET Framework. |
| **Evidence** | Microsoft .NET Framework 4.8  C:\Windows\Microsoft.NET\Framework\v4.0.30319\system.web.dll has not been patched.  Remote version : 4.8.4749.0  Should be : 4.8.4762.0 |

## VMware Tools Vulnerabilities.

|  |  |
| --- | --- |
| **Criticality** | **High** |
| **Synopsis** | A virtualization tool suite installed on the remote Windows host is affected by a privilege escalation vulnerability. |
| **Description** | The version of VMware Tools installed on the remote Windows host is 11.x prior to 11.2.6. It is, therefore, affected by a local privilege escalation vulnerability. An attacker with normal access to a virtual machine may exploit this issue by placing a malicious file renamed as 'openssl.cnf' in an unrestricted directory which would allow code to be executed with elevated privileges..  Following Vulnerabilities were identified due to the missing patches.   * Privilege Escalation (VMSA-2021-0013) * Authentication Bypass (VMSA-2023-0019) * Token Bypass (VMSA-2023-0024) * DoS (VMSA-2022-0029) |
| **Recommendation** | Upgrade to VMware Tools latest version |
| **Evidence** | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 11.2.6 |

## WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

|  |  |
| --- | --- |
| **Criticality** | **High** |
| **Synopsis** | The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability. |
| **Description** | The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:  *HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\Wintrust\*  *Config\EnableCertPaddingCheck*  *HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\*  *Wintrust\Config\EnableCertPaddingCheck*  An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host. |
| **Recommendation** | Add and enable registry value EnableCertPaddingCheck:  - HKEY\_LOCAL\_MACHINE\Software\Microsoft\Cryptography\Wintrust  \Config\EnableCertPaddingCheck  Additionally, on 64 Bit OS systems, Add and enable registry value  EnableCertPaddingCheck:   - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\  Cryptography\Wintrust\Config\EnableCertPaddingCheck  ***\*\*Please note that before making any changes, we recommend implementing them on the UAT server first, monitoring the progress, or seeking technical support if needed\*\**** |
| **Evidence** | Path : C:\Program Files\VMware\VMware Tools\  Installed version : 11.0.1.15528  Fixed version : 11.2.6 |

# Medium Vulnerabilities

## SSL Medium Strength Cipher Suites Supported (SWEET32)

|  |  |
| --- | --- |
| **Criticality** | **Medium** |
| **Synopsis** | The remote service supports the use of medium strength SSL ciphers. |
| **Description** | The remote host supports the use of SSL ciphers that offer medium strength encryption. Medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.  Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. |
| **Recommendation** | Reconfigure the affected application if possible to avoid use of medium strength ciphers. |
| **Evidence** | Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)   *Name Code KEX Auth Encryption MAC  ---------------------- ---------- --- ---- --------------------- ---  DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1*  The fields above are :   {ciphername}  {Cipher ID code}  Kex={key exchange}  Auth={authentication}  Encrypt={symmetric encryption method}  MAC={message authentication code}  {export flag} |

## TLS Version 1.0 Protocol Detection

|  |  |
| --- | --- |
| **Criticality** | **Medium** |
| **Synopsis** | The remote service encrypts traffic using an older version of TLS. |
| **Description** | The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| **Recommendation** | Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. |

## TLS Version 1.1 Deprecated Protocol

|  |  |
| --- | --- |
| **Criticality** | **Medium** |
| **Synopsis** | The remote service encrypts traffic using an older version of TLS. |
| **Description** | The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1  As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. |
| **Recommendation** | Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. |

## SMB Signing not required

|  |  |
| --- | --- |
| **Criticality** | **Medium** |
| **Synopsis** | Signing is not required on the remote SMB server. |
| **Description** | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. |
| **Recommendation** | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| **Evidence** | N/A |

# Additional Scans and Reports

FIT provides clients with a comprehensive Vulnerability Assessment Report that serves as a reference for remediating security vulnerabilities. This report includes detailed findings, risk assessments, and actionable recommendations to enhance the organization’s security posture. Additionally, FIT retains the raw scan results, such as Nessus files and full vulnerability scans, which can be made available upon request for clients requiring deeper technical insights.

