

Test Client Check

PENTEST REPORT

Executed by Cerberus Security

SUNDAY, DECEMBER 10, 2023





MODIFICATIONS HISTORY

Version	Date	Author	Description
0.1	12/10/2023	Daniel Scheidt	Initial Version
0.2	12/10/2023	Daniel Scheidt	Technical Details
1.0	12/10/2023	Daniel Scheidt	Finalization



TABLE OF CONTENTS

General Information	4
Scope	4
Organization	4
Executive Summary	5
Vulnerabilities summary	6
Technical Details	7
Disk Encryption Configuration	7
DHCPv6 Settings	8
Powershell Configuration	10
BIOS Hardening	12



GENERAL INFORMATION

SCOPE

Testcompany has mandated us to perform security tests on the following scope:

- WIN10X64.mcafeelab.local

ORGANIZATION

The testing activities were performed between 12/09/2023 and 12/10/2023.



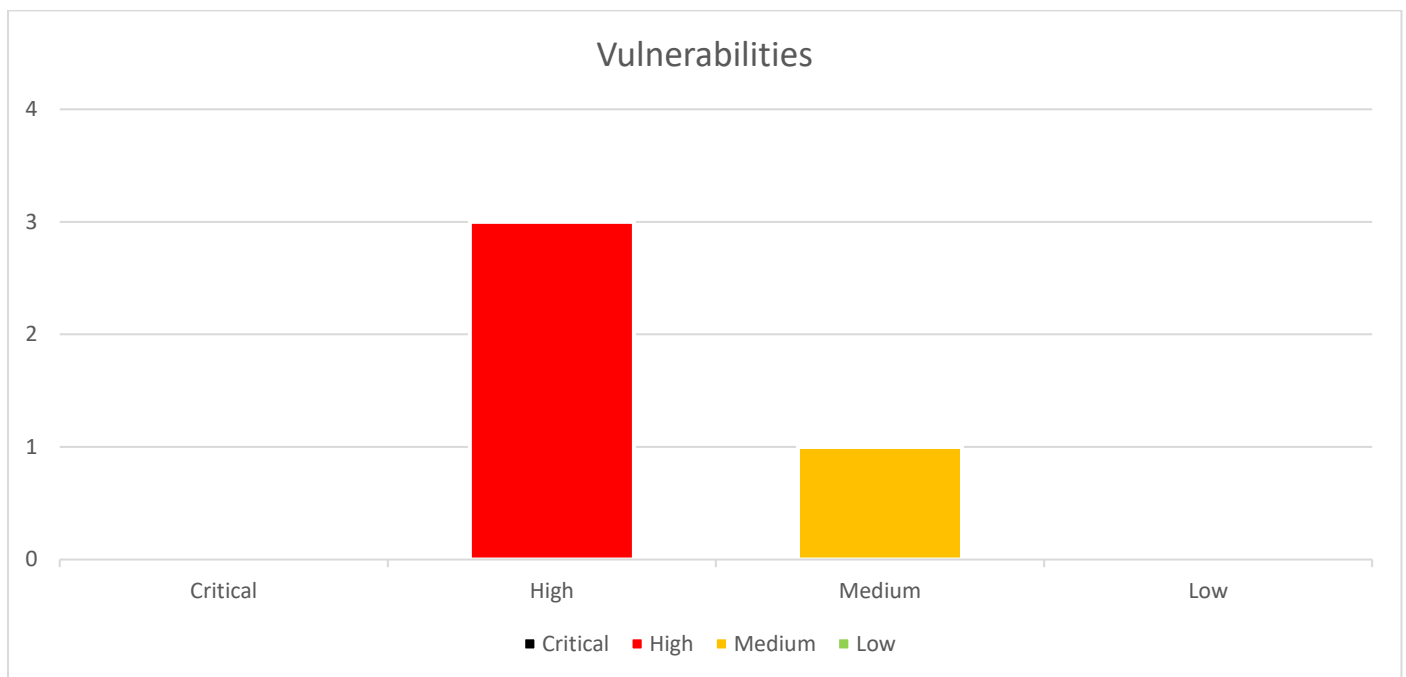
EXECUTIVE SUMMARY

Cerberus Security was tasked with conducting a Client Security Check for the exemplary client *WIN10X64*. The testing activities were performed between 12/09/2023 and 12/09/2023.

The goal is to get an overview of the overall security posture of the client systems used inside Testcompany. This should help the IT staff to identify weak points and enable them to fix and modify the current settings if needed.

The client was found to have lots of configurations wrongly set, that would allow an attacker gaining control over the device to run malware, execute code or implement persistence mechanisms. There is a lot of optimization potential that would mitigate or at least reduce the risks to execute certain attack tools or chains that adversaries tend to use in real world scenarios.

Tasks and efforts to reduce the attack surface vary highly, from little timely and resource efforts to larger projects that need more planning, time and people to tackle them. More info can be found in the details section of this report.





VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	Page	Vulnerability
High	7	Disk Encryption Configuration
High	8	DHCPv6 Settings
High	10	Powershell Configuration
Medium	12	BIOS Hardening



TECHNICAL DETAILS

DISK ENCRYPTION CONFIGURATION

SEVERITY	High
AFFECTED SCOPE	
DESCRIPTION	<p>Disk encryption is a security measure used to protect the data stored on a storage device, such as a hard drive or solid-state drive (SSD). It ensures that the data remains unreadable and inaccessible to unauthorized users even if the device is lost, stolen, or accessed without proper authorization.</p> <p>The primary purpose of disk encryption is to encrypt the entire contents of the disk, including the operating system, applications, and user data. It prevents unauthorized individuals from accessing or extracting sensitive information from the disk by encrypting it using a cryptographic algorithm.</p> <p>One method to enhance the security of disk encryption is through preboot authentication (PBA). PBA adds an additional layer of protection by requiring users to provide authentication credentials before the operating system boots up. This means that even if someone gains physical access to the device, they cannot bypass the encryption without providing the correct authentication.</p> <p>Preboot authentication typically involves a separate login screen or interface that prompts users to enter a password or other authentication factors, such as a PIN or biometric data (e.g., fingerprint or facial recognition). Only upon successful authentication will the device proceed to boot up the operating system and decrypt the disk.</p> <p>By combining disk encryption with preboot authentication, the data on the encrypted disk remains secure from unauthorized access. Even if an attacker manages to steal or gain physical access to the device, they would need to bypass the preboot authentication to gain access to the encrypted data.</p> <p>It is important to choose strong authentication credentials and regularly update them to maintain the security of the disk encryption. Additionally, ensuring the device's firmware and software are up to date helps protect against known vulnerabilities and ensures the effectiveness of the encryption and authentication mechanisms.</p>
OBSERVATION	There was no disk encryption present on the client, neither as 3rd party implementation nor with the built-in BitLocker software.

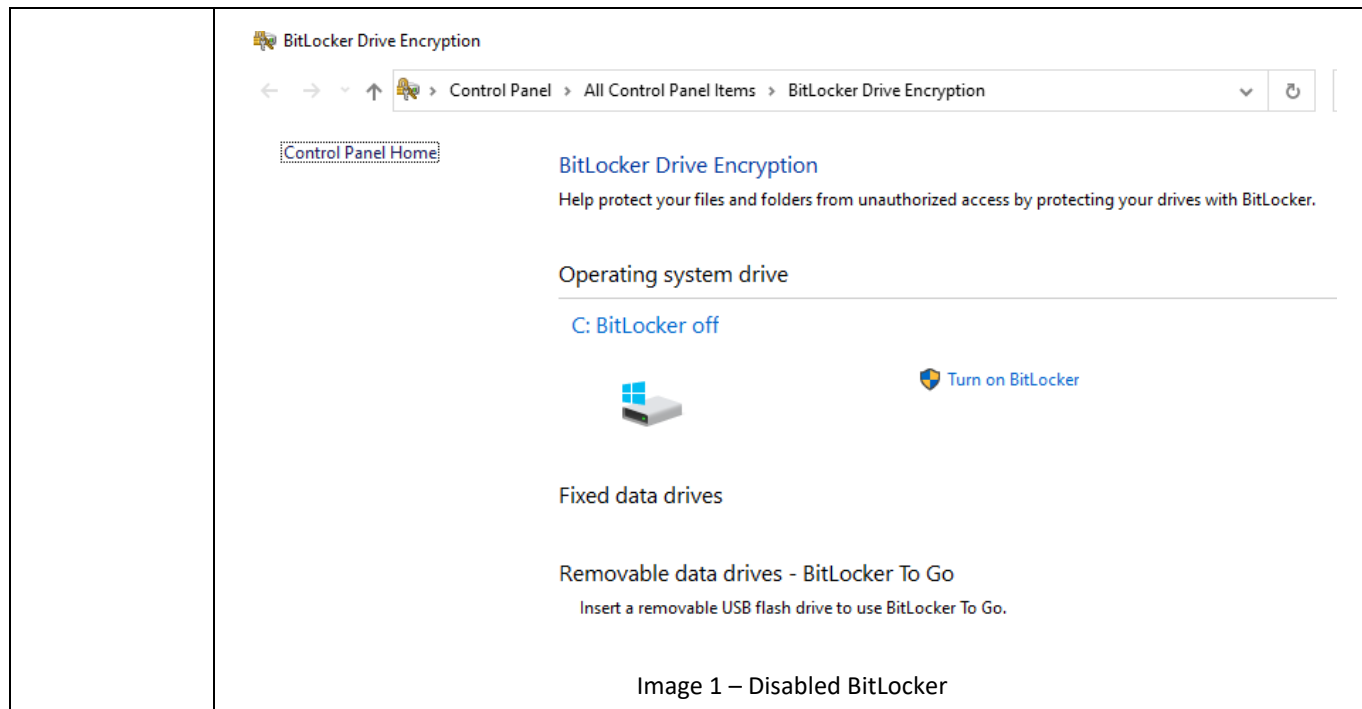


Image 1 – Disabled BitLocker

REMIEDIATION	<p>The implementation of a disk encryption should be considered to secure data at rest and prevent data loss in the case of a stolen device.</p> <p>If the encryption is meant to protect against sophisticated attacks, the TPM only mode for BitLocker would not be sufficient. One of the alternative solutions with an additional PIN or USB device should be taken into consideration[2].</p> <p>Another idea would be to make use of 3rd party applications that will give the user a SSO feeling that integrate with BitLocker.</p>
REFERENCES	<p>[1] https://luemmelsec.github.io/Go-away-BitLocker-you-are-drunk/</p> <p>[2] https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-countermeasures</p>

DHCPV6 SETTINGS

SEVERITY	High
AFFECTED SCOPE	
DESCRIPTION	<p>In DHCPv6, one of the potential attack vectors is related to the DHCPv6 offer process, specifically when configuring DNS servers. Here's an explanation of DHCPv6 attacks related to setting DNS servers via DHCP offers:</p> <ol style="list-style-type: none"> 1. Rogue DHCPv6 Server: An attacker can set up a rogue DHCPv6 server on the network to offer malicious DNS server addresses in the DHCPv6 response. When clients request DHCPv6 configuration, they may receive a DHCPv6 offer from the rogue server with DNS server addresses that the attacker controls. This can redirect the client's DNS queries to malicious DNS servers under the attacker's control.



2. DNS Spoofing: By providing malicious DNS server addresses in the DHCPv6 offer, an attacker can perform DNS spoofing. When clients use the offered DNS servers to resolve domain names, the attacker's DNS servers respond with false or malicious information. This can lead to users being redirected to malicious websites, phishing attacks, or manipulation of DNS responses to gain unauthorized access to sensitive information.
3. MITM Attacks: DHCPv6 DNS server configuration can also be exploited for Man-in-the-Middle (MitM) attacks. An attacker may intercept the DHCPv6 offer and modify the DNS server addresses to point to their own server. This enables the attacker to intercept DNS queries and responses, allowing them to monitor or manipulate the communication between the client and legitimate DNS servers.

Normally companies have a DHCPv4 server running but not one for DHCPv6. Modern Windows versions ship with IPv6 enabled, which takes precedence over IPv4. Hence out of the box these systems are likely to be vulnerable to the before mentioned attacks.

OBSERVATION

It was found that IPv6 is enabled on the client. The attacks mentioned in the description can hence be carried out against the client if an attacker happens to be on the same subnet.

```

Windows PowerShell
Windows IP Configuration

Host Name . . . . . : Win10x64
Primary Dns Suffix . . . . . : mcafeelab.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : mcafeelab.local
                                localdomain

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : mcafeelab.local
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-0C-29-0A-24-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::374e:e285:5c4a:2aa7%5(Preferred)
    IPv4 Address. . . . . : 10.55.0.152(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Sunday, December 10, 2023 2:50:55 PM
    Lease Expires . . . . . : Monday, December 18, 2023 2:50:56 PM
    Default Gateway . . . . . : 10.55.0.254
    DHCP Server . . . . . : 10.55.0.1
    DHCPv6 IAID . . . . . : 50334761
    DHCPv6 Client DUID. . . . . : 00-01-00-01-22-B5-58-A7-00-0C-29-0A-24-00
    DNS Servers . . . . . : 10.55.0.2
                                10.55.0.1
    NetBIOS over Tcpi. . . . . : Enabled
  
```

Image 2 – Enabled IPv6 on the Ethernet adapter connected to the domain

REMIEDIATION

- To mitigate the described attacks, the following measures can be implemented:
- Disable IPv6: If IPv6 is not required, it is recommended to disable the IPv6 interface on client systems. This can be done through network adapter settings or registry configurations.
 - Prefer IPv4 over IPv6: Network configurations can be adjusted to prioritize IPv4 connectivity over IPv6. This can be done by modifying network interface settings or network routing



	<p>configurations. In these cases the valid IPv4 configuration for e.g. DNS will "overrule" the rouge IPv6 DNS setting.</p> <ul style="list-style-type: none">• Exercise caution in disabling IPv6 on Servers: Microsoft advises against disabling IPv6 in server environments, as it may cause disruptions to critical functionalities such as Exchange or Domain Controllers. Careful consideration should be given before disabling IPv6 on servers.• Configure IPS/IDS Rules: Intrusion Prevention Systems (IPS) or Intrusion Detection Systems (IDS) can be configured with additional rules specifically designed to detect and mitigate DHCPv6 attacks. These rules should be regularly updated to address emerging threats.• Use Encrypted Connections: To prevent man-in-the-middle attacks, it is recommended to utilize encrypted connections wherever possible. This includes using secure protocols such as HTTPS for web communications and implementing VPNs (Virtual Private Networks) for secure remote access.• Specify Static Gateway and DNS Server: If IPv6 is necessary, it is advisable to manually configure and specify the gateway and DNS server addresses statically. This reduces the risk of DNS-related attacks by eliminating the reliance on DHCPv6 for network configuration.
REFERENCES	<p>https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/ https://www.blackhillsinfosec.com/mitm6-strikes-again-the-dark-side-of-ipv6/</p>

POWERSHELL CONFIGURATION

SEVERITY	High
AFFECTED SCOPE	
DESCRIPTION	<p>PowerShell is a task automation and configuration management framework developed by Microsoft, consisting of a command-line shell and associated scripting language built on the .NET framework. It was designed to provide a more efficient and effective way for Windows administrators to manage and automate various system administration tasks, including managing the Windows operating system and other Microsoft products such as Exchange, SharePoint, and SQL Server.</p> <p>PowerShell is often used by adversaries because it provides them with a built-in versatile tool for executing malicious scripts and commands, bypassing security controls, accessing sensitive information, and hiding their actions, making it an attractive tool for malicious actors.</p> <p>There are several steps that can be taken to harden the way PowerShell can act on a system or in specific user context:</p> <ul style="list-style-type: none">• Restrict the Language Mode <p>The PowerShell language mode determines the syntax, language elements, and behavior of PowerShell scripts, with the two main modes being "Full" and "Constrained" that can be used to restrict the capabilities of PowerShell scripts for security and administrative purposes.</p> <ul style="list-style-type: none">• Set an Execution Policy



The PowerShell execution policy is a security feature that determines what types of PowerShell scripts can run on a system and is used to help protect against malicious scripts by restricting the execution of scripts from unknown or untrusted sources.

- Uninstall old PowerShell versions

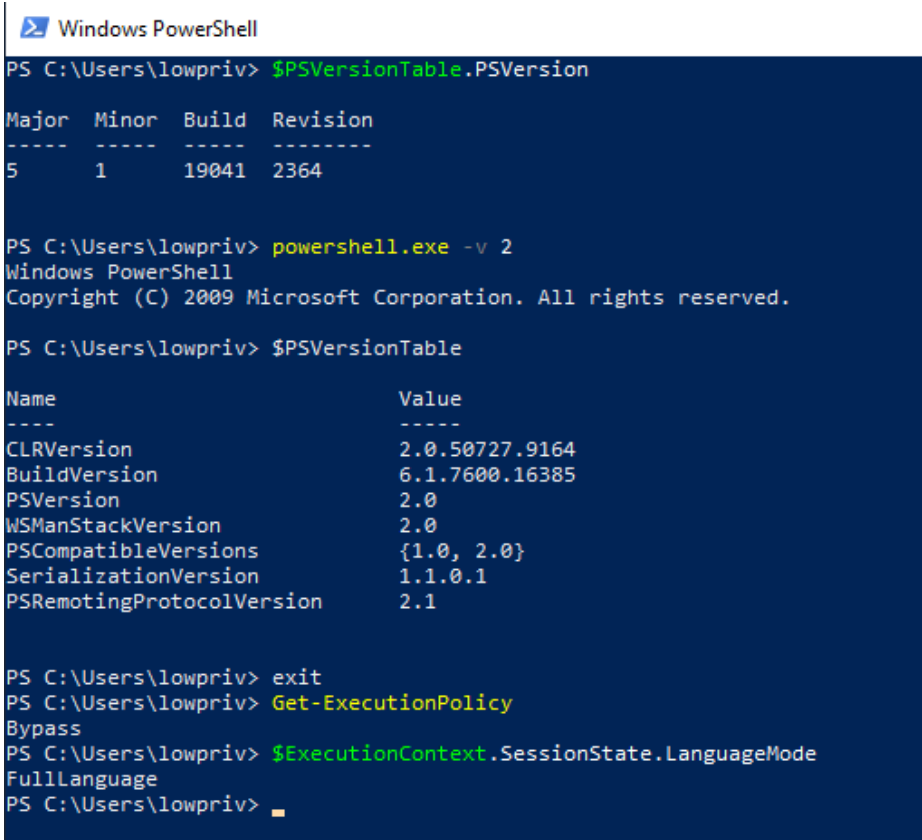
PowerShell version 5 and above has important built-in security features that make it safer to use in enterprise environments. For example, PowerShell v5 logs every script that is run, making it easier to trace the execution of malware.

These security features are not present in PowerShell v2.0, making it less secure, which at the same time makes it a lucrative alternative for attackers.

OBSERVATION

The investigation showed that:

- PowerShell v2 is available and can be used to bypass security features
- The language mode is set the *FullLanguage* allowing the users to execute PowerShell with the full commands available
- The execution policy is set to *Bypass*, effectively allowing to run all scripts on the device.



```

> Windows PowerShell
PS C:\Users\lowpriv> $PSVersionTable.PSVersion

Major  Minor  Build  Revision
-----
5      1      19041  2364

PS C:\Users\lowpriv> powershell.exe -v 2
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\lowpriv> $PSVersionTable

Name                               Value
----                               -
CLRVersion                         2.0.50727.9164
BuildVersion                        6.1.7600.16385
PSVersion                           2.0
WSManStackVersion                  2.0
PSCompatibleVersions               {1.0, 2.0}
SerializationVersion               1.1.0.1
PSRemotingProtocolVersion          2.1

PS C:\Users\lowpriv> exit
PS C:\Users\lowpriv> Get-ExecutionPolicy
Bypass
PS C:\Users\lowpriv> $ExecutionContext.SessionState.LanguageMode
FullLanguage
PS C:\Users\lowpriv>
  
```

Image 3 – PowerShell settings on the client

REMIEDIATION

Set the Language Mode to *Restricted*. This can be activated locally:

```
[Environment]::SetEnvironmentVariable('__PSLockdownPolicy', '4', 'Machine')
```

Or via Group Policies Objects:
Computer Configuration\Preferences\Windows Settings\Environment
 Set the Execution Policy to *AllSigned*.



	This can be done via GPO here: <i>Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell</i> Deactivate PowerShell v2.0 via GPO or remove it locally via the "Windows Features".
REFERENCES	https://adsecurity.org/?p=2604 https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-executionpolicy?view=powershell-7.3 https://learn.microsoft.com/en-us/powershell/scripting/learn/security-features?view=powershell-7.3 https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.3

BIOS HARDENING

SEVERITY	Medium
AFFECTED SCOPE	
DESCRIPTION	<p>The Basic Input/Output System (BIOS) is a firmware that is embedded in a computer's motherboard. It is responsible for initializing hardware components during the boot process and providing a basic set of instructions for the operating system to interact with the hardware.</p> <p>Securing the BIOS with a password is important for several reasons:</p> <ul style="list-style-type: none">• Unauthorized access prevention: Setting a BIOS password adds an extra layer of security to your computer system. It prevents unauthorized users from accessing and modifying critical BIOS settings, such as boot order, hardware configurations, and security features.• Protection against unauthorized booting: A BIOS password helps protect against unauthorized booting of the system from external devices, such as USB drives or optical media. It ensures that only authorized individuals can boot the system, reducing the risk of unauthorized access or malware infections.• Data protection: By securing the BIOS, you can help protect sensitive data stored on your computer. If someone tries to tamper with the BIOS settings or remove the hard drive, they will be unable to access the data without the BIOS password.• Preventing malicious firmware modifications: Securing the BIOS helps prevent unauthorized modifications to the firmware itself. Malicious actors could potentially modify the BIOS to install persistent malware or compromise the system's integrity. A BIOS password reduces the risk of such tampering.• Compliance and regulatory requirements: In certain industries or organizations, securing the BIOS with a password may be necessary to comply with industry regulations or internal security policies. It demonstrates a proactive approach to securing computer systems and protecting sensitive information. <p>It's important to note that while a BIOS password provides a level of security, it is not foolproof. Advanced attackers may still find ways to bypass or reset the BIOS password. However, setting a BIOS password is a recommended security practice that can help mitigate the risk of unauthorized access and protect system integrity.</p>



OBSERVATION	<p>The BIOS of the system in scope was not secured with a password. So, everyone with physical access to the device could tamper the settings.</p> <p>Additionally there was no disk encryption in place, which would allow an attacker to boot an OS from USB, reset the local Administrator password on the hard disk, and then gain access to all the company data stored on the device as privileged user.</p>
REMEDIATION	<p>A strong and unique password for each system should be used.</p>
REFERENCES	