

1BitofMemory

HackTheBox Findings Report:

**Arctic**

**Date: March 15th, 2020**

# Table of Contents

[Table of Contents 2](#_Toc35257029)

[Assessment Overview 3](#_Toc35257030)

[Assessment Components 3](#_Toc35257031)

[External Penetration Test 3](#_Toc35257032)

[Finding Severity Ratings 4](#_Toc35257033)

[Scope 5](#_Toc35257034)

[Scope Exclusions 5](#_Toc35257035)

[Client Allowances 5](#_Toc35257036)

[Executive Summary 6](#_Toc35257037)

[Attack Summary 6](#_Toc35257038)

[Security Strengths 6](#_Toc35257039)

[User Access Control 6](#_Toc35257040)

[Security Weaknesses 7](#_Toc35257041)

[Vulnerable Software 7](#_Toc35257042)

[Weak Password Policy 7](#_Toc35257043)

[Vulnerabilities by Impact 8](#_Toc35257044)

[External Penetration Test Findings 9](#_Toc35257045)

[**Vulnerable Software - ColdFusion (Critical) 9**](#_Toc35257046)

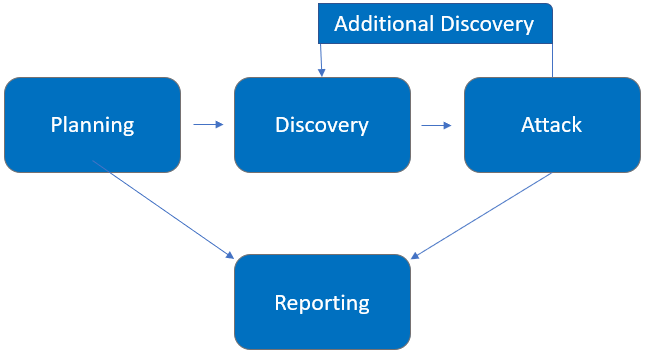
[**Vulnerable Operating System – Outdated Windows Server (Critical) 10**](#_Toc35257047)

[**Additional Reports and Scans (Informational) 12**](#_Toc35257048)

# Assessment Overview

Phases of penetration testing activities include the following:

* Discovery – Scanning and enumeration of given machine to gather information and identify vulnerabilities.
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

## External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. Independent penetration tester 1BitOfMemory performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# 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 | Details |
| External Penetration Test | 10.10.10.11 via VPN |

## Scope Exclusions

Per HackTheBox request, 1BitOfMemory does not perform any Denial of Service attacks during testing.

## Client Allowances

HackTheBox did not provide any allowances to assist the testing.

# Executive Summary

1BitOfMemory evaluated Arctic’s external security posture through an external network penetration test on March 15, 2020. By leveraging a series of attacks, 1BitOfMemory found critical level vulnerabilities that allowed full machine access. It is highly recommended that Arctic addresses these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Attack Summary

The following table describes how TCMS gained internal network access, step by step:

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 | Obtained valid admin password via SQL injection attack. | Discourage employees from using work e-mails and usernames as login credentials to other services unless necessary |
| 2 | Used valid credentials to upload and execute malware. | Synchronize valid and invalid account messages. |
| 3 | Performed privilege escalation tactics to be able to gain top-level access to the machine. | Update the operating system to the most current version. |

# Security Strengths

**User Access Control**

The user access control prevented unprivileged users from executing administrator tasks.

# Security Weaknesses

## Vulnerable Software

The ColdFusion software utilized is vulnerable and can be used to expose the administrator’s password hash.

## Weak Password Policy

The password hash obtained from the vulnerable software was quickly cracked as it did not have a high level of complexity.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

## External Penetration Test Findings

Vulnerable Software - ColdFusion (Critical)

|  |  |
| --- | --- |
| Description: | ColdFusion software leaked administrator credentials accessible to the public. |
| Impact: | Critical |
| System: | 10.10.10.11 |
| References: | <https://www.exploit-db.com/exploits/14641> |

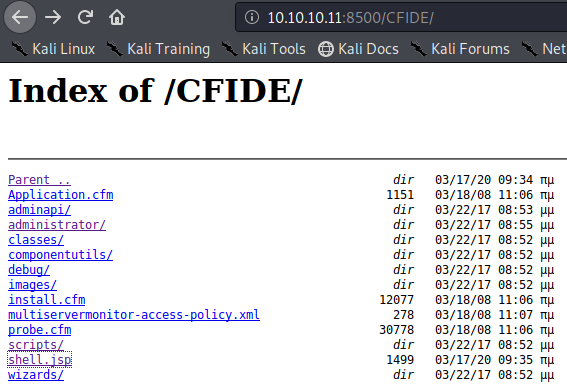
**Exploitation Proof of Concept**

1BitOfMemory was able to get the administrator’s password from ColdFusion software.



*Figure 1: Found credentials*

1BitOfMemory was able to upload a file to the server after logging in with these credentials. This was used to upload malware and gain remote access to the machine.



*Figure 2: shell.jsp was uploaded to the server*

1BitOfMemory was able to obtain the user flag from the resulting shell and leveraged privilege escalation techniques to gain administrator privileges.

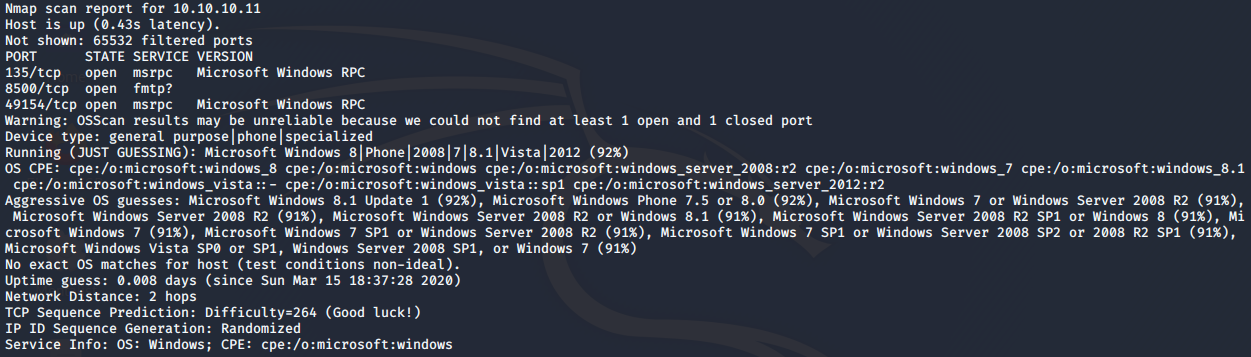
Vulnerable Operating System – Outdated Windows Server (Critical)

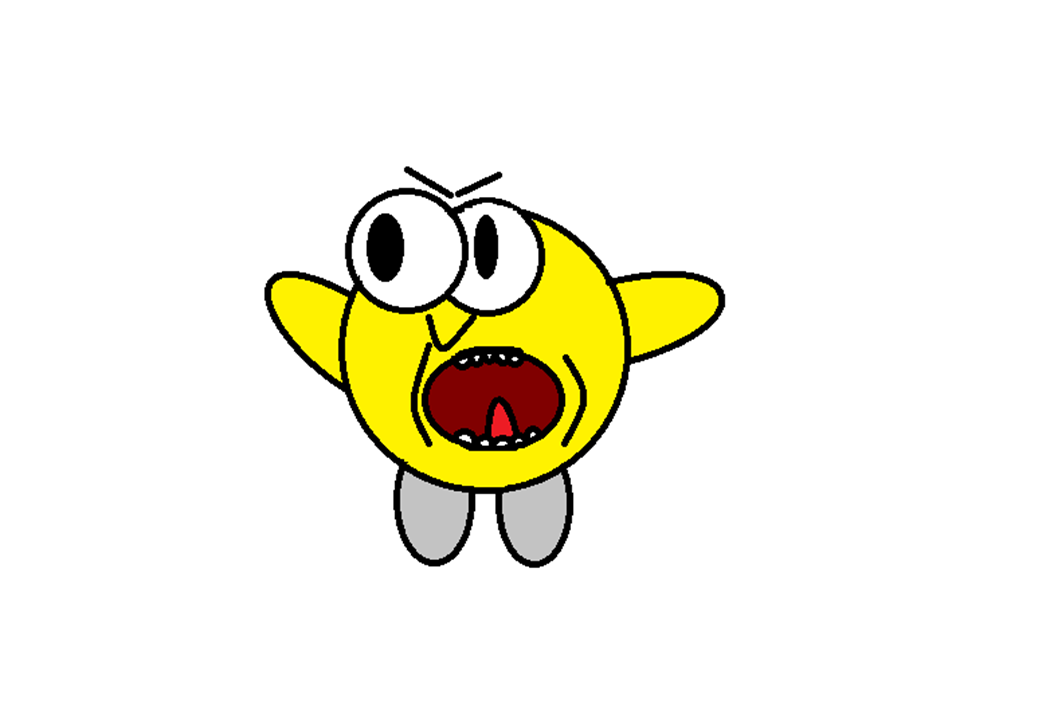
|  |  |
| --- | --- |
| Description: | The Windows Server utilized is vulnerable to a local exploit for privilege escalation. |
| Impact: | High |
| System: | 10.10.10.11 |
| References: | CVE-2015-1701 |

**Remediation**

|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: ColdFusion login with valid credentials did not require Multi-Factor Authentication (MFA). 1BitOfMemory recommends Arctic implements and enforces MFA across all external-facing login services.  Item 2: Patch or remove vulnerable software. The ColdFusion software has publicly known exploits that leak sensitive information. 1BitOfMemory recommends that the software be updated or replaced.  Item 3: Update the server’s operating system to the most current version. The current version allows a local exploit for privilege escalation. |

Additional Reports and Scans (Informational)





Last Page