BRACKISH SECURITY

External Penetration Test

PREPARED 12/15/24

DUNDER MIFFLIN, INC
PAPER COMPANY

Prepared For:

Michael Scott

Dunder Mifflin:

1725 Slough Ave, Scranton PA

Table of Contents

1. Summary of Changes

Change Information	Reason for Change	Date
Version 1.0	Initial Release	12/15/2024

Table 1: Summary of Changes

2. How to Use this Report

This document was prepared in accordance with cybersecurity best practices. Remediation recommendations, where applicable, are found within each related section. These recommendations specifically address the security concerns discussed in the respective sections. Wherever possible, screenshots are included to demonstrate methods and findings encountered during the period of performance of this test.

Consider that his report provides an external assessment of the cybersecurity vulnerabilities within your system(s) as identified by the Brackish Security testing team. It's crucial to understand that our evaluation is based on the information and access provided to us, and therefore may not encompass the full scope of your network and security protocols. We have rated the vulnerabilities according to our best judgment and industry standards.

However, it is essential for your internal security team to review each finding in the context of your specific environment. There may be existing mitigations or internal safeguards that we are not privy to, which could alter the severity or impact of these vulnerabilities. Thus, while this report serves as a valuable tool in identifying potential security risks, it should be used as a guide rather than a definitive statement of your system's security posture. Your team's internal knowledge and understanding of your systems are critical in accurately interpreting and effectively addressing the findings presented in this report.

This report represents a point-in-time snapshot of assets that underwent testing. In accordance with cybersecurity best practices, regular security assessments should be commissioned, especially after major changes to application source code or infrastructure. This report should not be considered absolute in nature as restrictions on time, economics, and resources contribute to a limited perspective that an assessment of this type provides.

3. Executive Summary

Dunder Mifflin (Client) engaged Brackish Security, LLC (Brackish) to perform an external penetration test. Testing commenced on 12/6/24 and continued through 12/13/24.

In total, there are five findings – highlighted by a Critical risk Cisco IOS Remote Code execution vulnerability that appears on CISA's list of known exploited vulnerabilities. Due to this vulnerability, the overall risk rating was initially determined to be Critical.

Table 2: Table of findings.

Finding	Severity
Cisco Smart Install Remote Code Execution: CVE-2018-0171	Critical
Weak Cisco Configuration Passwords	Medium
Microsoft IIS Short Name File and Directory Enumeration	Low
Externally Accessible SNMP Service	Informational
Breach Data – Clear Text Credentials	Informational

During the discovery and exploitation of the aforementioned bug, testers exfiltrated a Cisco configuration file and were able to crack the credentials found within the configuration. The obtained passwords are six characters in length, which is below the recommended character size, and represents a notable weakness.

Testers also found a Microsoft Short Name File and Directory Enumeration bug on two hosts that could potentially allow sensitive information to be disclosed, though testers found that no sensitive files were present.

Additionally, testers found multiple credential leaks containing credentials of possible Dunder Mifflin employees. These credentials are included in separate files.

Fortunately, during the process of testing, the Client was notified of the Cisco vulnerability and immediately implemented a fix, which was verified as effective shortly thereafter by the testing team. These timely actions reduce the overall risk to **Medium**.

4. Positive Observations

Brackish Testers attempted to lightly brute force several of the login pages identified and the Solarwinds Serv-U login page banned the tester's IP address after roughly 30 requests. Although there are numerous ways an attacker can circumvent these controls, it does slow down an attacker or bot activity.

Figure 1: Solarwinds Serv-U Login Page prior to brute-forcing

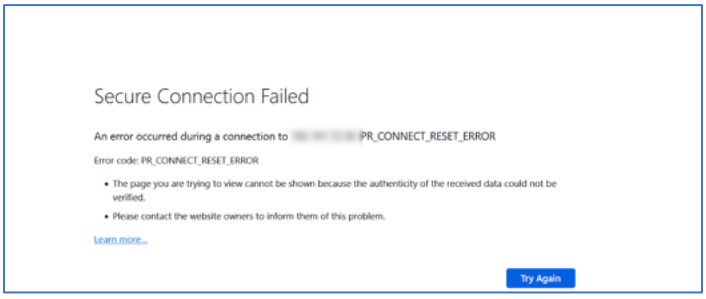

Figure 2: Solarwinds Serv-U Login Page inaccessible after brute-forcing attempts

5. Key Recommendations

Regular Firmware Updates

Establish a routine for regularly updating the firmware and auditing configurations of all devices. This helps in addressing vulnerabilities that are newly discovered and patched.

Vulnerability Management Program

Implement a comprehensive vulnerability management program that includes regular scans, assessments, and prompt remediation of identified vulnerabilities.

6. Scope

External IP Addresses
[External IP Range]
[External IP Range]
[External IP Range]

Table 3: Assets that were in scope for active testing.

7. Brief Methodology Overview

Testing commenced by utilizing common scanning tools such as Nessus, Nmap, and Nuclei to discover live hosts and running services. Both Nessus and Nuclei indicated no noteworthy vulnerabilities, and minimal running services.

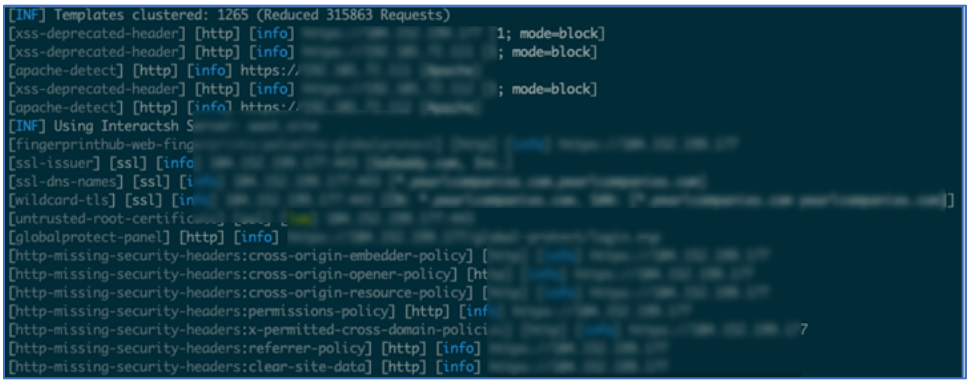

Figure 3: Nuclei output indicating no notable vulnerabilities.

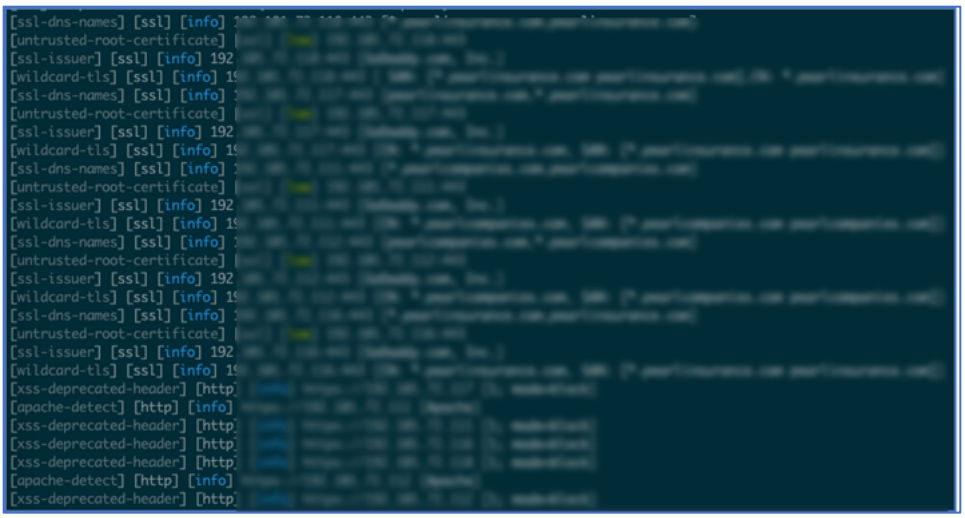

Figure 4: Additional Nuclei output indicating no notable vulnerabilities.

Nmap indicated several UDP ports were open and hosting standard infrastructure services, along with TCP ports that indicated web applications. Testers attempted limited brute forcing of these endpoints with no success. Searches for vulnerabilities related to running software such as Serv-U and Mitel turned up nothing of note.

Figure 5: Various open UDP ports.

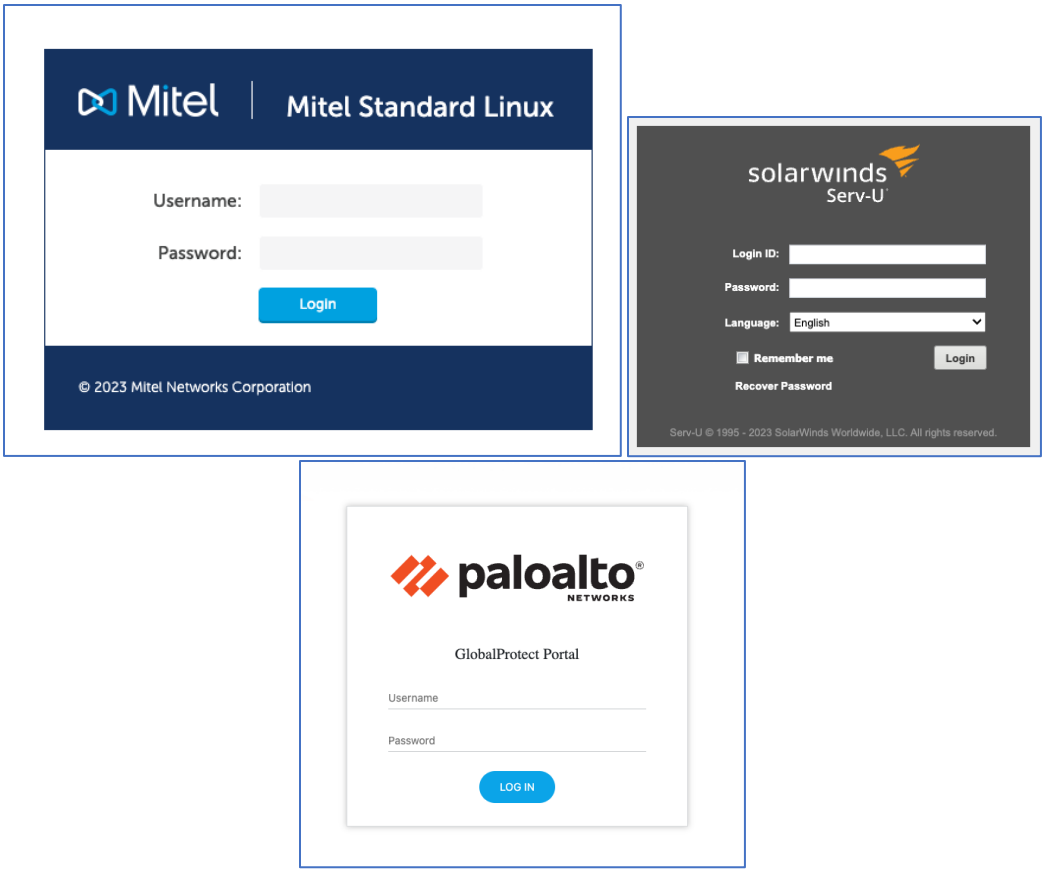

Figure 6: Various login panels discovered during testing.

SSLScan was utilized to verify TLS configurations of all HTTPS servers discovered. No weakly configured or misconfigured servers were found.

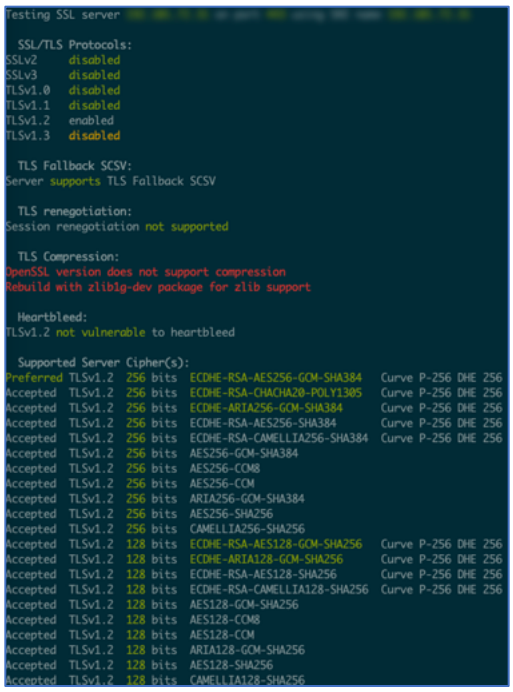

Figure 7: Example SSLScan from an in-scope host detailing protocols and cipher suites in use.

Testers did find five hosts with Cisco Smart Install enabled. Three of these hosts are acting as directors and two as clients. The Clients were determined to be vulnerable to Critical risk vulnerability – CVE-2018-0171 - as detailed in the findings section of this report. The configuration files from these devices were obtained and their passwords were cracked due to their insufficient length – also noted in a finding.

Numerous tools were used during testing, a sample of which are found in the table below.

Tool	Description	URL
Burp Suite	Web security testing toolkit	Portswigger
GoWitness	Open-source web page screenshotting tool	Github
Nessus	Commercial Vulnerability Scanner	Nessus
Nmap	Network mapping tool	Nmap
Nuclei	Open-source vulnerability scanner	Github
SpiderFoot	Open-source intelligence gathering tool	Github
SSLScan	Scanner to detect SSL/TLS settings	SSLScan
Burp Suite	Web security testing toolkit	Portswigger

Table 4: Tooling utilized during both phases of testing.

8. Primary Findings

Below is a table of the finding with their associated severities. Where applicable, vulnerabilities are scored with the Common Vulnerability Scoring System (CVSS) version 3.1, a well-respected, open framework that provides a precise and consistent methodology for rating the severity of security vulnerabilities. CVSS v3 allows us to evaluate the exploitability, impact, and other characteristics of a vulnerability in an objective manner, resulting in a score ranging from 0 to 10. This score is then translated into a qualitative representation (such as Low, Medium, High, or Critical) which provides an initial baseline understanding of the severity of each finding in a standardized context.

ID	Finding	Severity	CVSS
DNDR-01	Cisco Smart Install Remote Code Execution: CVE-2018-0171	Critical	9.4
DNDR-02	Weak Cisco Configuration Passwords	Medium	4.9
DNDR-03	Microsoft IIS Short Name File and Directory Enumeration	Low	2.9
DNDR-04	Externally Accessible SNMP Service	Informational	N/A
DNDR-05	Breach Data – Clear Text Credentials	Informational	N/A

Table 5 : Findings and severities

DNDR-01 – Cisco Smart Install Remote Code Execution: CVE-2018-0171

Current Rating	CVSS
Critical	**9.4**
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H	

Description:

Testers found multiple hosts vulnerable to CVE-2018-0171, a vulnerability in the Smart Install feature of Cisco IOS Software. This is a CISA known exploited vulnerability. Testers were able to exfiltrate the device's configuration file, but attackers can also use this vulnerability to perform denial of service or remote code execution attacks.

Figure 8: Checking for affected hosts.

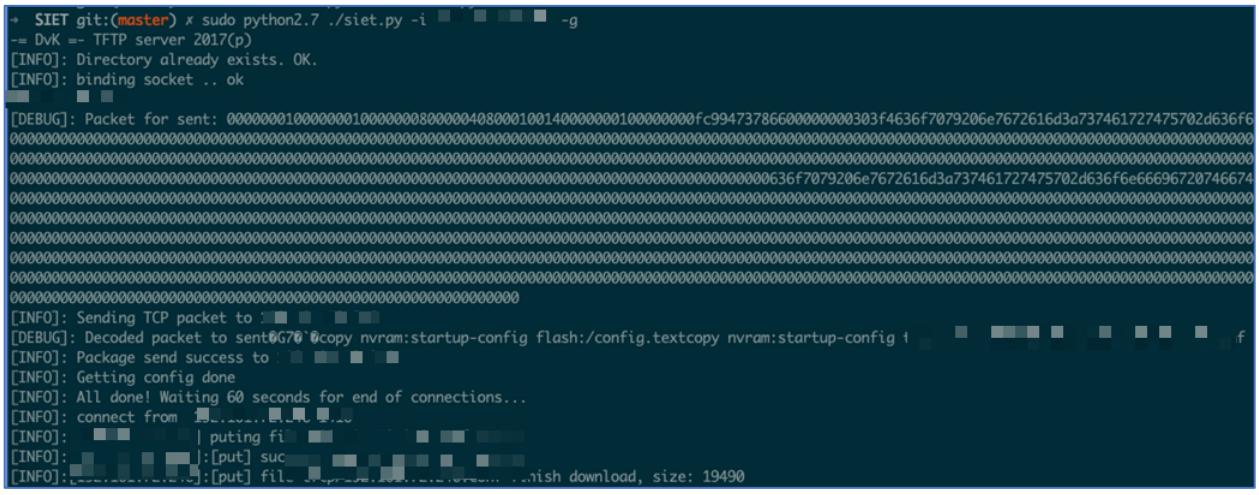

Figure 9: Testers running the exploit.

```
!
! Last configuration change at 17:08:38 UTC Thu Oct 19 2023 by lee.clements
! NVRAM config last updated at 17:09:10 UTC Thu Oct 19 2023 by lee.clements
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname NY_c4500x
!
boot-start-marker
boot system flash bootflash:cat4500e-universalk9.SPA.03.09.00.E.152-5.E.bin
license boot level entservices
boot-end-marker
!
!
vrf definition OOB-Management
 !
 address-family ipv4
 exit-address-family
!
vrf definition mgmtVrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 5 $1$qsR2$WYU.s3e73S20OXLb9CaoA/
!
username admin privilege 15 password 7 15053D5A053373
aaa new-model
!
!
aaa group server radius AD-RADIUS
 server name AlbDC2
 server name PiaDC2
 ip vrf forwarding OOB-Management
 ip radius source-interface Vlan20
!
aaa authentication login default local enable
aaa authentication login AD-RADIUS group AD-RADIUS local
aaa authorization console
aaa authorization exec default local if-authenticated
aaa authorization exec AD-RADIUS group AD-RADIUS local
```

Figure 10: Partial output of a retrieved configuration file.

Dunder Mifflin was immediately notified of this issue and took action to remediate. Subsequent testing indicated that the fix was successful, as pictured below.

```
➜  SIET git:(master) ✗ sudo python2.7 ./siet.py -i [redacted] -g
-= DvK =- TFTP server 2017(p)
[INFO]: Directory already exists. OK.
[INFO]: binding socket .. ok
[ERROR]: Couldn't connect to [redacted], exit.
```

Figure 11: Testers were no longer able to connect to the devices.

Affected Hosts:

The service is found on TCP port 4786 of the following hosts:

- [IP address] - Director Service

- [IP address] - Director Service
- [IP address] - Director Service
- [IP address] – Client Service (Vulnerable to CVE-2018-0171)
- [IP address] – Client Service (Vulnerable to CVE-2018-0171)

Recommendation:

- Disable this feature if it is not needed.
- Apply Cisco IOS updates that address this vulnerability.
- Change any credentials found within the configuration files of these devices.

Reference:

https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20180328-smi2.html

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi

https://blog.talosintelligence.com/cisco-coverage-for-smart-install-client/

https://nvd.nist.gov/vuln/detail/cve-2018-0171

DNDR-02 – Weak Cisco Configuration Passwords

Current Rating	CVSS
Medium	**4.9**
Vector: AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/CR:H/IR:H/AR:H/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:L/MI:N/MA:N	

Description:

After obtaining Cisco appliance configuration files, testers were able to crack the admin user and EXEC mode passwords associated with the devices and found them to be six characters in length.

The limited length of these passwords drastically reduces their complexity, making them highly vulnerable to brute-force attacks, especially with modern tools that utilize GPU acceleration, capable of cracking such passwords extremely quickly. Additionally, they are more prone to dictionary attacks, as people often use predictable patterns and common substitutions, making these short passwords easier to guess. To mitigate this risk, it's crucial to enforce a minimum

password length of at least fourteen characters and to ensure multi-factor authentication is in use on supported endpoints.

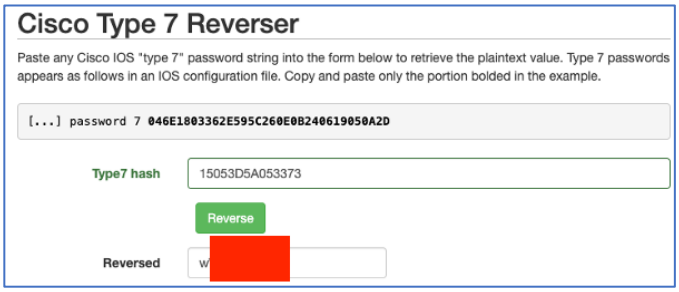

Figure 12: Cisco admin user password reversing.

Figure 13: Testers were able to crack the EXEC mode password.

Recommendation:

Brackish recommends fourteen-character passwords be used for user accounts and infrastructure devices.

References:

https://cwe.mitre.org/data/definitions/521.html

DNDR-03 – Microsoft IIS Short Name File and Directory Enumeration

Current Rating	CVSS
Low	**2.9**
Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C/CR:L/IR:X/AR:X/MAV:N/MAC:H/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N	

Description:

Testers found multiple hosts to be vulnerable to IIS short name file and directory enumeration. This is a method used to discover the short 8.3 format filenames in a Windows environment.

By using this enumeration method, an attacker can uncover the 8.3 filenames of files and folders. This can reveal the existence of files or directories that might not be obvious from their long filenames, potentially disclosing sensitive information or the presence of certain applications or files.

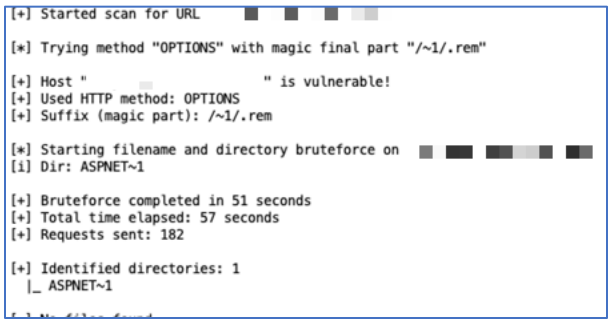

Figure 14: Enumerating short file names on this host.

Fortunately, testers were only able to enumerate a single directory on the server. In other cases, this method can divulge sensitive files and directories allowing an attacker to further attacks or access files they previously did not know existed.

Affected Hosts:

https:// [IP address]

https://webchat.dundermifflin.com/ [IP address] – No files or directories enumerated.

Recommendation:

The primary method to address this issue is to disable the creation of 8.3 filenames on the NTFS volumes. This can be done using the **fsutil** command on Windows.

```
fsutil 8dot3name set <VolumeID> 1
```

Alternatively, you can make changes in the Windows registry to disable 8.3 name creation. This approach is more complex and requires careful handling as incorrect changes in the registry can adversely affect system stability.

- Navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem*.
- Modify the *NtfsDisable8dot3NameCreation* entry to *1*.

Reference:

https://soroush.me/blog/2012/06/microsoft-iis-tilde-character-vulnerabilityfeature-short-filefolder-name-disclosure/

https://brackish.io/iis-short-file-name-enumeration/

DNDR-04 – Externally Accessible SNMP Service

Current Rating	CVSS
Informational	**N/A**

Description:

Testers found the hosts listed below publicly expose SNMPv3. Public exposure of SNMPv3 can lead to unauthorized access and potential exploitation, as it allows attackers to target and potentially compromise network devices remotely. Additionally, while SNMPv3 includes encryption and better authentication, it is still susceptible to network scanning and brute-force attacks, which can lead to the disclosure of sensitive network information and infrastructure details, compromising the overall security posture of the network.

Affected Hosts

[IP address]	[IP address]	[IP address]	[IP address]	[IP address]

Recommendation:

Investigate if operations require this service to be exposed and disable or place behind a firewall if not.

DNDR-05 – Breach Data – Clear Text Credentials

Current Rating	CVSS
Informational	**N/A**

Description:

Valid credentials belonging to their Dunder Mifflin employees were found listed on DeHashed.com, a database known for hosting compromised online credentials. This finding is indicative of a potential security breach, posing a substantial risk of unauthorized system access. Testers were able to validate the credentials were valid by entering them into Dunder Mifflin's Microsoft Office 365 portal. Testers were prevented from authenticating by MFA.

Brackish security testers also identified the username and password of the account 'admin@dundermifflin.com to be associated with breached data. Testers were unable to authenticate these credentials.

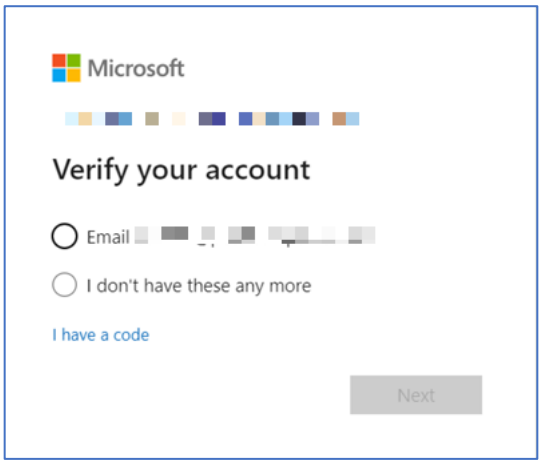

Figure 15: Valid credentials for user account dwight.schrute@dundermifflin.com prompting for MFA token

Figure 16: Breach credentials for dwight.schrute@dundermifflin.com

Figure 17: Breach credentials for 'admin@dudermifflin.com'

Recommendation:

Enforce a mandatory password rotation of all user accounts. Conduct user awareness training for all users on the importance of not using work email for personal usage. Do not use admin account to sign up for third party services.

9. CVSS v3.0 Reference Table

Qualitative Rating	CVSS Score
None/Informational	N/A
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Table 6 : Common Vulnerability Scoring System Version 3.0