Vulnerability Assessment
With
Penetration Testing

For

شركة جدارة
لتحصيل ديون جهات التمويل
Jadarah Funders Debt Collection Co.

Oct 10, 2024

Cyper Space's Red Team has taken great care to ensure the accuracy, relevance, and completeness of the information presented in this report. The findings reflect our comprehensive analysis up to the conclusion of this engagement. We hope this report provides clear insights and valuable recommendations to strengthen your security posture.

Document Details

Document's Title	Jadarah VAPT Report
Version	1.0
Classification	CONFIDENTIAL
Document's Author	Cyper Space Red Team
Issued at	10 Oct 2024
Document's State	FINAL

Recipient List / Distribution Group

Copy History Number	1
Name	Misfer Al-Ajmi, IT Department
Location	Riyadh – Dammam branch Road

Classification

Type	Authorized	Controlled	Restricted	Validity	Period
External	Yes				3 months
Internal		Yes			UNLIMITED

1. VAPT Context & Objective

This report outlines the results of the second external Vulnerability Assessment and Penetration Testing (VAPT) performed on JADARAH Company's specified internet-facing assets. The assessment focused on evaluating the security posture of these assets as part of JADARAH's broader security review process.

The specific objectives of this assessment are to:

- Capture a detailed snapshot of the current security state of JADARAH's in-scope assets, including publicly accessible servers, services, and network components.
- Verify that the existing security measures offer sufficient protection against common and targeted threats, while identifying any critical or easily exploitable vulnerabilities.
- Provide precise, actionable recommendations to mitigate identified risks and strengthen the security of these assets.

The VAPT was conducted by emulating a skilled threat actor, aiming to exploit vulnerabilities in JADARAH's internet-facing systems. This simulated attack sought to determine whether a remote attacker could gain unauthorized access or compromise these assets, as well as assess the potential damage or data exposure resulting from any security weaknesses.

The findings in this report reflect the vulnerabilities and risks observed during the testing period and may not represent any subsequent changes or improvements made to the systems.

1.1 VAPT Scope

Asset Type	URL
Web Apps	**https://192.168.100.251/jadarh**
IP Range	**192.168.100.1** to **192.168.101.254**
Network Subnet	**/23**

1.2 VAPT Timeline

The timeline for the local site starts active and end as below.

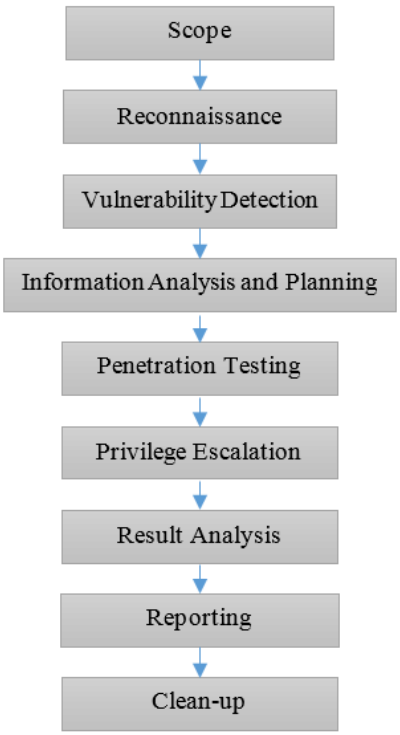
Start Date/Time	End Date/Time
25/09/2024	**09/10/2023**

1.2 VAPT Approach

The VAPT technical process utilized a black box reactive hybrid approach, leveraging both automated and manual testing techniques to ensure thorough coverage, high-quality results, and greater consistency. This approach, designed to mimic the perspective of an external attacker with no prior knowledge of the environment, involved the following stages:

1. **Reconnaissance**: Gathering information about the in-scope assets to understand the attack surface and identify potential entry points.
2. **Vulnerability Detection**: Using automated tools to scan for known vulnerabilities and weaknesses in the exposed systems and services.
3. **Manual Testing**: Conducting in-depth, hands-on testing to validate the findings from the automated scans and uncover additional vulnerabilities that automated tools may miss.
4. **Pen-testing and Privilege Escalation**: In this phase, the identified vulnerabilities were actively exploited to assess their potential impact. The focus was on determining whether unauthorized access could be gained and, if so, whether it was possible to escalate privileges. This step involved.
5. **Result Analysis**: Assessing the consequences of successful exploitation, including data exposure, privilege escalation, and persistence within the system.
6. **Reporting**: Compiling and documenting the findings, including detailed recommendations for mitigating or resolving identified vulnerabilities.

And practically it is summed up below as in figure below:



1.3 Toolbox

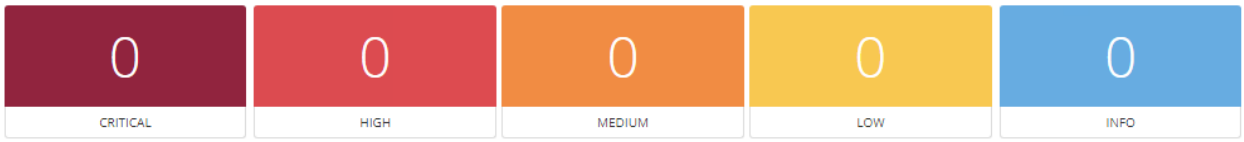
The toolbox used during this VAPT includes open source and commercial tools.

B.2 II. VAPT of Finding

2.1 Graphical Summary and detailed of Results

Based on the analysis and statistics, the overall information security threat and risk rating for the in-scope assets has been determined to be **Critical**. This rating reflects the severity and potential impact of the identified vulnerabilities, indicating that immediate action is required to mitigate the associated risks and protect the assets from potential exploitation detailed as below or Summery:

Detailed:



Summery:



- **Severity & Threat Rating**

Critical: A Vulnerability that have direct threat to key business processes and which, if exploited would allow malicious native code to execute, potentially without a user being aware.

High: A vulnerability that have also a direct threat to key business processes which, if exploited would compromise data security, potentially allowing access to confidential data, or could compromise processing resources in a user's system.

Medium: A vulnerability that have indirect threat to key business processes or partial threat to business processes and which is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.

Low: No direct threat exists. Vulnerability may be exploited using other vulnerabilities.

Informational: This finding does not indicate vulnerability just some info about usual and regular application registers.

2.0 Metric & Risk rating

Score Risk Asset Evaluation System

The **ScoRisk Asset Evaluation System** is designed to assess and manage the security posture of assets within an organization. It involves a structured approach to evaluate the risks associated with various assets and determine their overall threat and risk ratings.

A is Positive Grade (green) and **E** is Negative grade(red).
These ratings are based on certain criteria.

Key components of the system typically include:

1. **Asset Identification**: Cataloging all assets within the scope of evaluation, including hardware, software, and data.
2. **Risk Assessment**: Evaluating the potential threats and vulnerabilities associated with each asset, considering factors such as exposure, sensitivity, and criticality.
3. **Threat and Risk Rating**: Calculating the overall threat and risk rating based on the identified vulnerabilities and their potential impact. Ratings can range from Low to Critical.
4. **Mitigation Strategies**: Recommending and implementing measures to address

identified risks and vulnerabilities, aiming to reduce the overall risk rating.

5. **Continuous Monitoring**: Regularly reviewing and updating the risk assessments to reflect changes in the threat landscape and asset conditions.
6. **Reporting**: Documenting the findings and risk ratings, providing actionable insights and recommendations for improving the security posture of the assets.

Score RISK of Asset = **6 and C**

Probability	Severity 1	Severity 2	Severity 3	Severity 4	Severity 5
Very High	6	12	18	36	72
High	4	7	14	28	56
Medium	3	5	10	20	40
Low	2	3	6	12	24
Very Low	1	1	2	4	8

ScoRISK Grades		
A	Excellent ranking	Suitable for Firewalls, filtering devices, security devices, highly hardened servers, banking and payment services
B	Good ranking	Suitable for frontal web services. Some common servers (webmail, company web server…)
C	Low ranking	
D	Poor ranking	
E	Very poor ranking	

2.1 Strengths and Weaknesses

In general, the attack surface of the JADARAH in-scope assets was assessed to be relatively minimal. However, the assessment identified several security threats that pose a significant risk to these assets. Notably, the following enumerated potential weaknesses were found, which could compromise the security posture of the in-scope assets:

Strong points:

- **Firewall Protection**: The tested in-scope asset is safeguarded by an active firewall by ESET Firewall endpoint along with UTM hardware FortiGate, which provides a crucial layer of defense by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. This protection helps to block unauthorized access and potential threats from reaching the asset.

- **Brute Force and Guessing Attacks**: The in-scope assets are not vulnerable to guessing or brute force attacks, indicating robust protection against unauthorized access attempts and ensuring that common attack vectors for credential or key guessing are mitigated.

- **Services and Ports**: The services and ports operating on the in-scope assets are predominantly filtered rather than permissive. This configuration restricts unnecessary exposure and limits the potential attack vectors available to external threats.

Weak points:

- **invalid SSL/TLS Implementations**: Issues were discovered with SSL/TLS implementations, which could compromise the confidentiality and integrity of data transmitted between clients and servers.

- **Unauthenticated Endpoints Disclose Secrets and Default Credentials**: Certain unauthenticated endpoints which use default passwords on IP phones like admin, admin was found to expose sensitive information or default credentials, potentially allowing unauthorized access to critical systems or data.

- **Outdated patches of ESXi**: The VMware ESXi installation is not up-to-date with the latest patches, leaving it vulnerable to known exploits and security risks the root cause of non-patched is not connected to internet.

- **Insufficient Logging and Monitoring**: Inadequate logging and monitoring of the VOIP server can hinder the detection and response to suspicious activities or security incidents.

In-Scope Assets Card: Hassel

URL / IP / Port	Asset Model	Situation Report	Threat Severity
https://192.168.100.251	Web Application	Vulnerability an attack is likely	

1. Severity

- Likely

2. Vulnerability Type

Unauthenticated:

- The system is susceptible to successful **brute force attacks** due to insufficient protection measures against repeated password guessing attempts.
- SSL/TLS not applied on IP only and there is no DNS.
- Multiple Command Injection Vulnerabilities in Grandstream Products
- SSL Medium Strength Cipher Suites Supported (SWEET32)
- SSL Certificate Signed Using Weak Hashing Algorithm

3. Description

Brute Force Attack Vulnerability: The Hassel application running on the server with IP address 172.16.0.50 is susceptible to successful brute force attacks. This vulnerability arises due to inadequate protection measures against repeated password guessing attempts, which could allow unauthorized access to the system.

Unencrypted SMTP Configurations: The Hassel server's SMTP configurations are set up to use a non-encrypted server method. This configuration exposes email communications to potential interception and unauthorized access, as data transmitted via SMTP is not protected by encryption.

SSL/TLS Implementation Issues: SSL/TLS is not applied to IP communications on this server. The encryption is only active for DNS traffic, leaving other communications vulnerable to eavesdropping and man-in-the-middle attacks. This lack of comprehensive encryption can compromise the security of sensitive data transmitted between clients and the Hassel server.

4. Impact

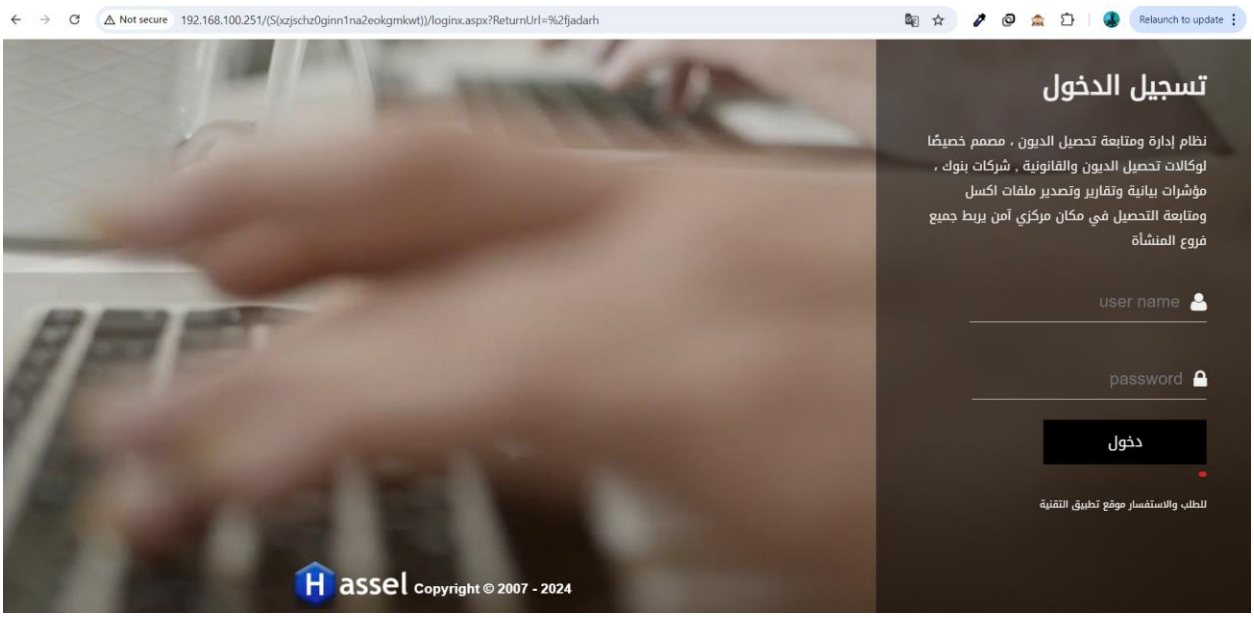
Brute Force Attack Vulnerability: Successful brute force attacks could allow unauthorized individuals to gain access to the Hassel application, potentially leading to unauthorized administrative control, data breaches, or service disruption. This could compromise the confidentiality, integrity, and availability of the communication systems.

Unencrypted SMTP Configurations: The lack of encryption in SMTP configurations poses a risk of email interception and unauthorized access to email content. Sensitive information transmitted via email could be exposed to malicious actors, leading to potential data leaks, privacy breaches, and exploitation of confidential communications.

SSL/TLS Implementation Issues: The absence of SSL/TLS encryption for IP communications means that data transmitted between clients and the Hassel server is vulnerable to eavesdropping and tampering. Attackers could intercept and manipulate communication, potentially leading to the theft of sensitive information or unauthorized access to the system. This exposure could also facilitate man-in-the-middle attacks, where attackers can intercept and alter communications between the server and its clients.

5. POC

Below some screenshot prove of concept of the Vulnerability



The application running on static IP nor than domain name server.

Discovery Stage

1 Screenshot of Passive OSINT

OSINT is not applicable to this asset as it operates within an internal network and is not exposed to external sources.

Port Scan

The active port scanning determined that there are only four ports (80,22,443,541,5090) were found to be allowed from outside on the origin system and some ports for Internal VOIP.

nmap -p- 192.168.100.0/23

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 21:19 Arab Standard Time
Nmap scan report for 192.168.100.1
Host is up (0.034s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE  SERVICE
113/tcp closed ident
443/tcp open   https
541/tcp open   uucp-rlogin
MAC Address: 04:D5:90:0B:03:22 (Fortinet)

Nmap scan report for 192.168.100.2
Host is up (0.0099s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
8000/tcp open  http-alt
MAC Address: E8:A0:ED:73:7A:28 (Hangzhou Hikvision Digital Technology)

Nmap scan report for 192.168.100.3
Host is up (0.015s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
8000/tcp open  http-alt
MAC Address: E8:A0:ED:73:79:70 (Hangzhou Hikvision Digital Technology)

Nmap scan report for 192.168.100.4
Host is up (0.014s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
8000/tcp open  http-alt
MAC Address: E8:A0:ED:73:79:CA (Hangzhou Hikvision Digital Technology)
```

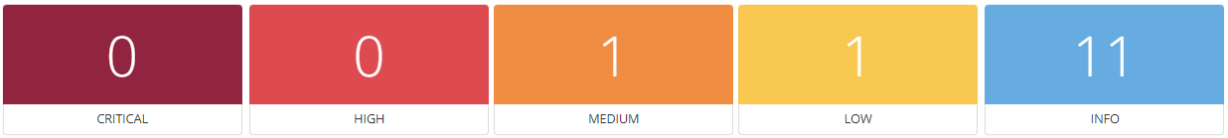
Vulnerability Assessment Stage

No significant security issues were detected during the course of the vulnerability scanning.

Screenshots of Vulnerability Scan

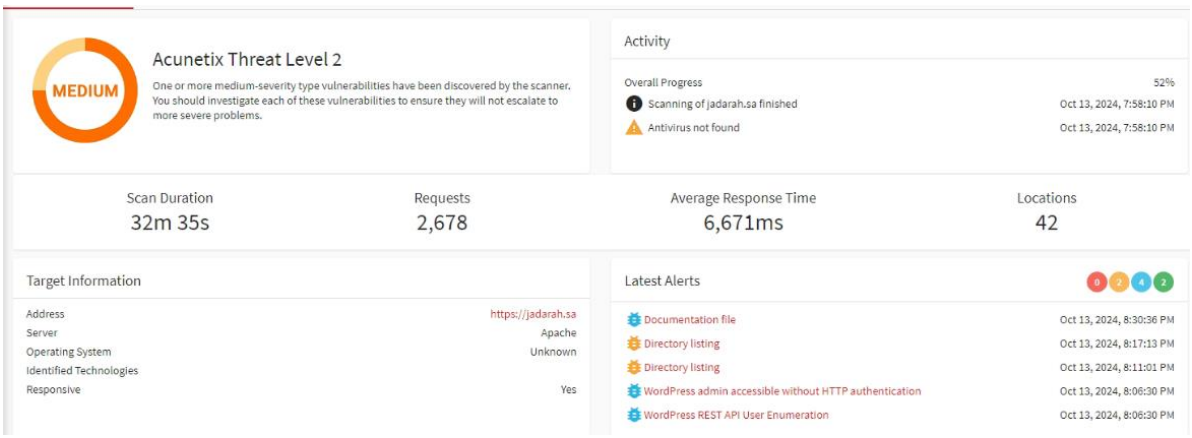
1. Nessus

192.168.100.11



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	5.0*	-	-	12218	mDNS Detection (Remote Network)
LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type

2. Acunetix



- **Screenshots of Attack & Exploitation Process**
  The executed automated and manual attacks reveal additional security weaknesses that can be exploited to bypass and compromise the security of the internet facing asset.

  Automate Attack
  Nothing was found for SQL Injection.

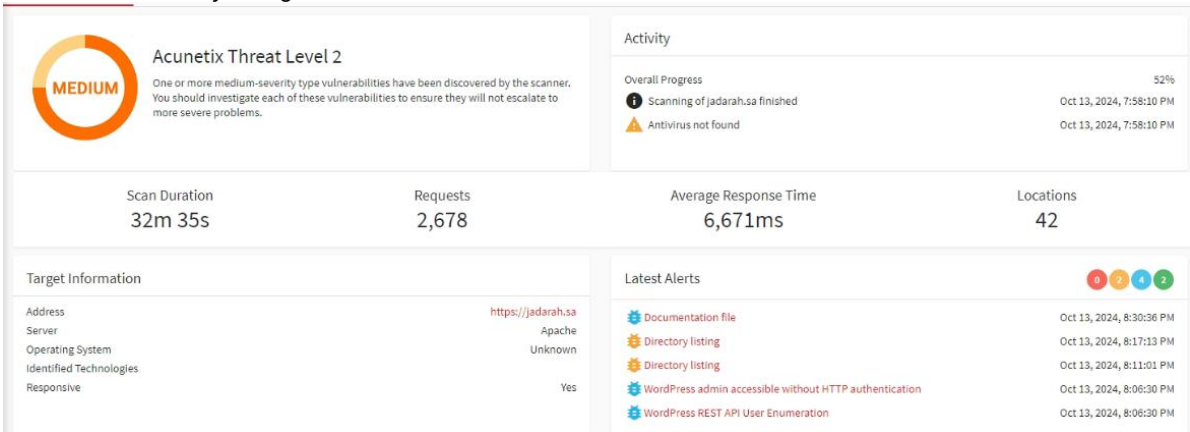
Nothing was found for SQL Injection.

Spider results

URL	METHOD	PAGE TITLE	PAGE SIZE	STATUS CODE
https://jadarah.sa/	GET	قريباً	4.35 KB	200
https://jadarah.sa/wp-content/plugins	GET		0	200
https://jadarah.sa/wp-content/plugins/coming-soon-maintenance-mode/	GET	Index of /wp-content/plugins/coming-soon-maintenan	1.93 KB	200
https://jadarah.sa/wp-content/plugins/coming-soon-maintenance-mode/admin	GET	Index of /wp-content/plugins/coming-soon-maintenan	1.07 KB	200
https://jadarah.sa/wp-includes/js	GET	Index of /wp-includes/js	20.59 KB	200
https://jadarah.sa/wp-includes/js/jquery	GET	Index of /wp-includes/js/jquery	4.08 KB	200

Acunetix

Issues with Directory listing



Manual Attack

```python
import requests

# URL where the SQL injection is possible
url = "http://192.168.100.251/jadarh"

# SQL Injection payload
payload = "1' OR '1'='1"

# Send the malicious request
params = {'id': payload}
response = requests.get(url, params=params)

# Print the response
print(response.text)
```

After run the script The Network or Firewall Blocking the Connection

SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MSSQL server version for the right syntax to use near '' OR 1=1--' at line 1

Recommendation

To mitigate the risk of a **brute force attack** on the Hassel application, here are some key recommendations:

1. Enable Multi-Factor Authentication (MFA)

- **Why**: MFA adds an extra layer of security, making it harder for attackers to gain access even if they have compromised the password.
- **How**: Ensure that MFA is enabled for all accounts, particularly administrative ones.

2. Implement Strong Password Policies

- **Why**: Weak passwords make brute force attacks easier.
- **How**: Enforce strong password requirements (e.g., minimum length, complexity, periodic changes). Use passphrases where possible.

3. Account Lockout Mechanism

- **Why**: Locking accounts after a certain number of failed login attempts can stop brute force attacks.
- **How**: Configure the system to lock accounts after 3-5 failed attempts and notify the administrator of these events.

4. Limit Login Attempts

- **Why**: Throttling login attempts slows down brute force attacks.
- **How**: Implement rate-limiting to reduce the number of login attempts per minute from a single IP address.

5. Use Captchas on Login Pages

- **Why**: Captchas prevent automated tools from performing brute force attacks.
- **How**: Integrate captchas on login interfaces, especially after several failed attempts.

6. Enable IP Whitelisting

- **Why**: Restricting access to the hassel application from trusted IP addresses reduces exposure.
- **How**: Allow only authorized IP addresses to access the system, particularly for administrative accounts.

7. Monitor and Analyze Login Activity

- **Why**: Detecting unusual login attempts can help in stopping attacks early.
- **How**: Set up logging and monitoring for login attempts and use SIEM tools to identify suspicious behavior.

8. Network Segmentation

- **Why**: Isolating critical systems can prevent lateral movement within the network after a successful brute force attack.
- **How**: Use VLANs or subnetting to segment sensitive systems and limit access only to authorized users.

9. Regular Patching and Updates

- **Why**: Unpatched vulnerabilities can be exploited in brute force attacks.
- **How**: Ensure the Hassel application, operating systems, and underlying infrastructure are updated regularly.

10. Use a Web Application Firewall (WAF)

- **Why**: A WAF can filter and block malicious traffic, including brute force attempts.
- **How**: Deploy a WAF in front of the Hassel application to monitor and block suspicious login requests.

Implementing these recommendations will significantly reduce the risk of brute force attacks on the Hassel system and enhance its security.

1. Enforce TLS Encryption (STARTTLS)

- **Why**: STARTTLS encrypts SMTP communication, preventing the interception of emails during transmission.
- **How**: Enable STARTTLS on your mail servers and ensure that both incoming and outgoing emails use encryption. Update your server to prefer or enforce TLS for email transport.

2. Implement SMTP over SSL (SMTPS)

- **Why**: SMTPS encrypts the entire communication channel between email servers, protecting sensitive data.
- **How**: Configure your email server to use SMTPS (usually on port 465) to ensure emails are transmitted securely.

3. Enforce Opportunistic TLS for All SMTP Connections

- **Why**: Opportunistic TLS provides encryption whenever possible, without breaking communication with non-TLS-enabled servers.
- **How**: Configure the SMTP server to attempt TLS on all outbound connections and require it for sensitive communications.

4. Update DNS Records for DANE (DNS-Based Authentication of Named Entities)

- **Why**: DANE ensures that the SMTP server's TLS certificate is legitimate, protecting against Man-in-the-Middle (MITM) attacks.
- **How**: Use DNSSEC and publish DANE records to ensure your SMTP servers are using valid TLS certificates.

5. Disable Plaintext Authentication Methods

- **Why**: Plaintext authentication allows attackers to capture credentials, increasing the risk of unauthorized access.
- **How**: Disable plaintext methods like LOGIN and PLAIN unless they are secured with TLS, and prefer encrypted methods like CRAM-MD5.

6. Enforce SMTP Authentication (SMTP AUTH)

- **Why**: SMTP AUTH ensures that only authenticated users can send emails, reducing the risk of email spoofing.
- **How**: Require SMTP authentication for all outgoing emails, ensuring only authorized users can send emails via the SMTP server.

7. Regularly Rotate and Update SSL/TLS Certificates

- **Why**: Expired or weak certificates weaken email security.
- **How**: Ensure SSL/TLS certificates are up-to-date and issued by a trusted Certificate Authority (CA). Set reminders for certificate renewal.

To address SSL/TLS implementation issues for IP communications with the Hassel server, follow these recommendations:

1. Implement SSL/TLS for All Communications

- **Why**: SSL/TLS encrypts data in transit, protecting it from eavesdropping and tampering.
- **How**: Configure the Hassel server to use SSL/TLS for all communications, including client-server and server-server connections. Ensure that all network traffic is encrypted.

2. Obtain and Install a Valid SSL/TLS Certificate

- **Why**: A valid certificate ensures that encrypted connections are secure and trusted.
- **How**: Acquire an SSL/TLS certificate from a reputable Certificate Authority (CA). Install and configure the certificate on your Hassel server.

Note: The assets tested within the internal network have not been exposed to the public. The reported findings have been reviewed and addressed by the JADARAH team.

In-Scope Assets Card: Network Scan

URL / IP / Port	Asset Model	Situation Report	Threat Severity
192.168.100.1-192.168.101.254	IP Address	Vulnerable	

1. Severity and vulnerability type

- **Critical**

- ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)
- VMware ESX / ESXi Unsupported Version Detection
- ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)

- **High**

- ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)
- ESXi < 7.0 Reflected Denial of Service
- SSL Medium Strength Cipher Suites Supported (SWEET32)
- ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)

2. Description

1. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)
Severity: **Critical**
Description: According to its version, the installation of VMware ESX or ESXi on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

2. ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)
Severity: **Critical**
Description: The remote VMware ESXi host is version 6.5 or 6.7 and is affected by a cross-site scripting (XSS) vulnerability in virtual machine attributes due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker with access to modify the system properties of a virtual machine from inside the guest OS can exploit this, by inserting script-related HTML in the system properties and having a user view the system properties from the ESXi Host Client, to execute arbitrary script code in a user's ESXi Host Client session.

3. VMware ESX / ESXi Unsupported Version Detection
Severity: **Critical**
Description: According to its version, the installation of VMware ESX or ESXi on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

4. ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)
Severity: **High**
Description: The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by a remote code execution vulnerability. OpenSLP as used in ESXi (7.0 before ESXi70U1c-17325551, 6.7 before ESXi670-202102401-SG, 6.5 before ESXi650-202102101-SG) has a heap-overflow vulnerability. A malicious actor residing within the same network segment as ESXi who has access to port 427 may be able to trigger the heap-overflow issue in OpenSLP service resulting in remote code execution.

5. ESXi < 7.0 Reflected Denial of Service
Severity: **High**
Description: The remote VMware ESXi host is less than version 7.0 and is affected by a reflected denial of service vulnerability:
- The Service Location Protocol (SLP, RFC 2608) allows an unauthenticated, remote attacker to register arbitrary services. This could allow the attacker to use spoofed UDP traffic to conduct a denial-of-service attack with a significant amplification factor. (CVE-2023-29552)

6. SSL Medium Strength Cipher Suites Supported (SWEET32)
Severity: **High**
Description: The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

7. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)
According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities.

- A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's VMX process running on the host. (CVE-2020-4004)

- A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An authenticated, local attacker with privileges within the VPM process can exploit this, when chained with CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005)

3. Impacting

1. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)
- **Impact**: The lack of support means that these versions will no longer receive security patches, leaving them vulnerable to known and future security issues. Any vulnerabilities discovered after the end of support will remain unpatched, exposing the system to potential breaches, malware infections, and unauthorized access. This could lead to data breaches, service disruptions, and unauthorized control over virtual machines.

2. ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)
- **Impact**: The cross-site scripting (XSS) vulnerability can allow an attacker to inject malicious scripts into the ESXi Host Client session. If a legitimate user views the system properties containing the malicious script, the attacker can execute arbitrary code in that user's session. This could lead to session hijacking, unauthorized access to sensitive data, and potentially further compromising the ESXi server.

3. VMware ESX / ESXi Unsupported Version Detection
- **Impact**: Similar to point 1, running an unsupported version leaves the system vulnerable to unpatched security risks. Any newly discovered vulnerabilities won't be addressed by the vendor, increasing the risk of exploitation. This could result in the compromise of the ESXi host, unauthorized access to virtual machines, and loss of sensitive data.

4. ESXi 6.5 / 6.7 / 7.0 Remote Code Execution (VMSA-2021-0002)
- **Impact**: The heap-overflow vulnerability in the OpenSLP service can allow a malicious actor to execute arbitrary code remotely. This could lead to complete

control over the ESXi host, allowing the attacker to manipulate virtual machines, steal data, or disrupt services. The vulnerability is particularly dangerous because it can be exploited remotely without user interaction.

5. ESXi < 7.0 Reflected Denial of Service (DoS)

- **Impact**: The reflected denial-of-service vulnerability can be exploited by an unauthenticated attacker to overwhelm the system using spoofed UDP traffic. This could cause significant service disruptions, rendering the ESXi host or its virtual machines unavailable. If exploited, it could result in extended downtime, loss of productivity, and potential financial losses.

6. SSL Medium Strength Cipher Suites Supported (SWEET32)

- **Impact**: Supporting medium-strength cipher suites (such as 3DES) makes the system vulnerable to attacks that exploit weak encryption. This could allow attackers to intercept or decrypt communications between clients and the ESXi host. Sensitive information like credentials or session tokens could be exposed, leading to unauthorized access and data theft.

7. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)

- **Impact**:
  - **CVE-2020-4004 (Use-after-free in XHCI USB controller)**: This vulnerability allows a local attacker with administrative privileges on a virtual machine to execute code on the ESXi host. This could lead to complete control of the host from within a compromised virtual machine.
  - **CVE-2020-4005 (Privilege escalation)**: When combined with CVE-2020-4004, this allows an attacker to escalate privileges, giving them full administrative control over the ESXi host. The impact could include unauthorized access to sensitive systems, modification of virtual machines, and disruption of services.

Discovery Stage

Passive OSINT

OSINT is not applicable to this asset as it operates within an internal network and is not exposed to outside.

Port Scanning

The active port scanning determined that there are ports were found to be allowed from outside on the origin system (below shown IPs with open ports).

- ✓ 192.168.100.1

```
Nmap scan report for 192.168.100.1
Host is up (0.011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
113/tcp closed ident
443/tcp open   https
541/tcp open   uucp-rlogin
MAC Address: 04:D5:90:0B:03:22 (Fortinet)
```

- ✓ 192.168.100.2

```
Nmap scan report for 192.168.100.2
Host is up (0.012s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
8000/tcp open  http-alt
MAC Address: E8:A0:ED:73:7A:28 (Hangzhou Hikvision Digital Technology)
```

- ✓ 192.168.100.3

```
Nmap scan report for 192.168.100.3
Host is up (0.0092s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
8000/tcp open  http-alt
MAC Address: E8:A0:ED:73:79:70 (Hangzhou Hikvision Digital Technology)
```

- ✓ 192.168.100.4

```
Nmap scan report for 192.168.100.4
Host is up (0.010s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
8000/tcp open  http-alt
MAC Address: E8:A0:ED:73:79:CA (Hangzhou Hikvision Digital Technology)
```

- ✓ 192.168.100.100

```
Nmap scan report for 192.168.100.100
Host is up (0.013s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5985/tcp open  wsman
7070/tcp open  realserver
MAC Address: 00:0C:29:79:1B:09 (VMware)
```

- ✓ 192.168.100.230

```
Nmap scan report for 192.168.100.230
Host is up (0.0067s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3261/tcp open  winshadow
5000/tcp open  upnp
5001/tcp open  commplex-link
5357/tcp open  wsdapi
5510/tcp open  secureidprop
MAC Address: 90:09:D0:60:5D:AD (Synology Incorporated)
```

✓ 192.168.100.254

```
Nmap scan report for 192.168.100.254
Host is up (0.0056s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5051/tcp open  ida-agent
5060/tcp open  sip
5985/tcp open  wsman
7070/tcp open  realserver
9001/tcp open  tor-orport
MAC Address: 00:0C:29:94:E0:3B (VMware)
```

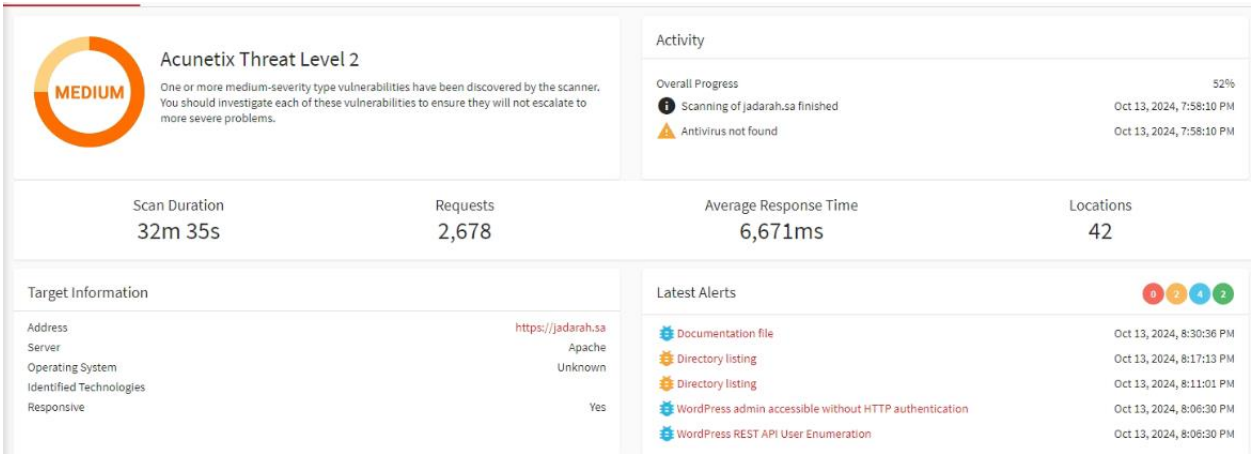
Vulnerability Assessment Stage

No significant security issues were detected during the course of the vulnerability scanning.

Screenshots of Vulnerability Scan

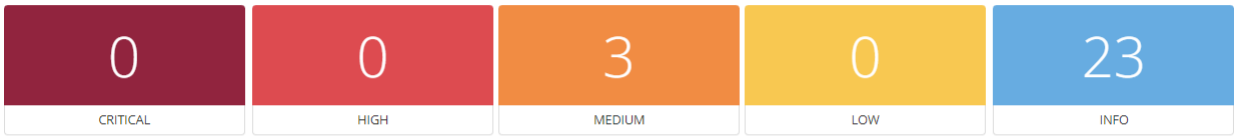
1. **Acunetix**

✓ Jadarah.sa



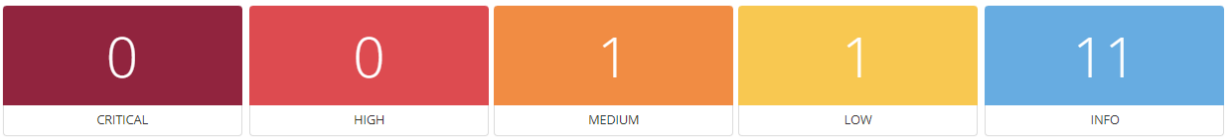
2. Nessus

192.168.100.1



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type

192.168.100.11



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	5.0*	-	-	12218	mDNS Detection (Remote Network)
LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type

192.168.100.14

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	1	17

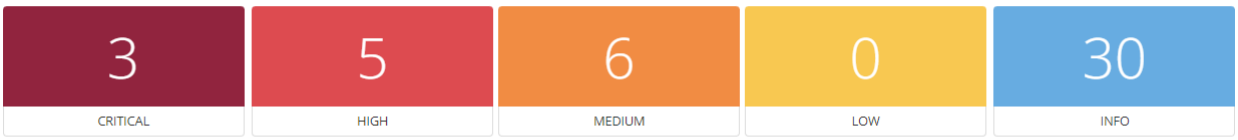
Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.0*	-	-	12218	mDNS Detection (Remote Network)
LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)

192.168.100.33

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	2	32

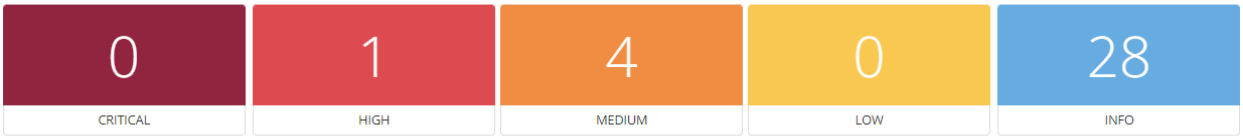
Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	N/A	-	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type

192.168.100.250



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
CRITICAL	9.8	-	-	151665	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014)
CRITICAL	9.3	-	-	138475	ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)
CRITICAL	10.0	-	-	56997	VMware ESX / ESXi Unsupported Version Detection
HIGH	8.8	-	-	168828	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0030)
HIGH	8.8	-	-	146827	ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)
HIGH	8.2	-	-	143221	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)
HIGH	7.8	-	-	158494	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2022-0004)

192.168.100.251



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
HIGH	7.5	-	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)

The full scan attached with VAPT Report as html file.

- **Attack & Exploitation Stage**

Screenshots of Attack & Exploitation Process

The executed automated and manual attacks reveal additional security weaknesses that can be exploited to bypass and compromise the security of the internet facing asset

1. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014) - Unsupported Version
Attack Scenario: An attacker, aware that the target ESXi version is no longer supported, could launch various exploits against known vulnerabilities. Without vendor-released patches, the host becomes an attractive target for attacks like remote code execution, privilege escalation, or even denial-of-service (DoS). An attacker could scan for outdated ESXi versions, find one, and exploit one or more of these vulnerabilities. With no security updates, the system becomes increasingly vulnerable over time, allowing an attacker to gain full control of the hypervisor, compromise VMs, or disrupt critical business services.
2. ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)
Attack Scenario: An authenticated attacker with guest OS access could insert malicious script code in virtual machine attributes. When an administrator later views the VM's system properties using the ESXi Host Client, the attacker's script executes in the administrator's browser session. This could be used to steal the administrator's session, perform actions on behalf of the admin (like shutting down VMs), or inject further malware into the environment. The attacker could escalate their privileges or compromise sensitive systems, leading to data theft or service disruption.
3. VMware ESX / ESXi Unsupported Version Detection
Attack Scenario: In a scenario where ESXi versions have reached their end of support, an attacker could target known, unpatched vulnerabilities for those versions. The attacker could scan for such installations and use publicly available exploits to gain unauthorized access or launch attacks like privilege escalation or denial-of-service. Since the host is no longer receiving security updates, the attacker has a broad surface to exploit, possibly gaining control over the hypervisor, executing arbitrary code, or crashing critical virtualized services, causing widespread business disruption.
4. ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)
Attack Scenario: In this case, an attacker inside the same network segment could exploit the OpenSLP heap-overflow vulnerability by sending specially crafted packets to port 427, where the Service Location Protocol (SLP) runs. This heap-overflow attack could allow the attacker to execute arbitrary code on the ESXi host, leading to full control of the host and its virtual machines. From here,

the attacker could exfiltrate data, install malware, or disrupt services by shutting down or corrupting VMs. If multiple ESXi hosts are in the same network, the attacker could pivot to compromise other parts of the environment.

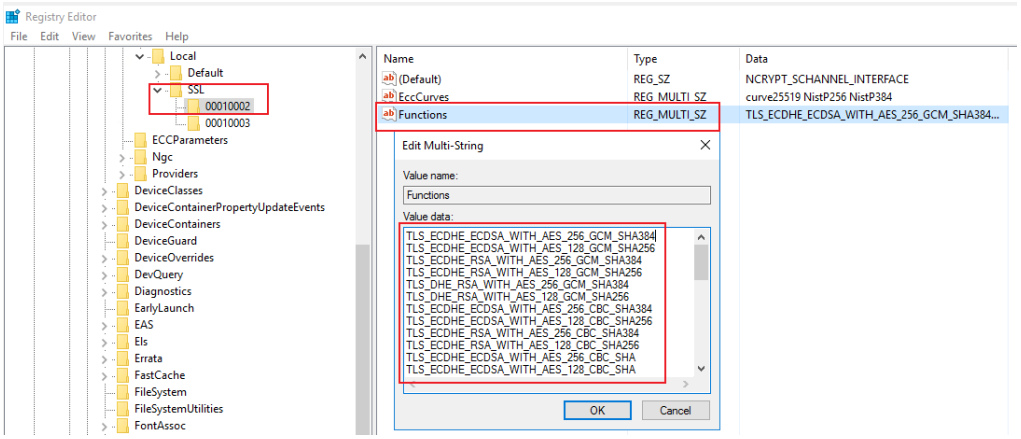
5. ESXi < 7.0 Reflected Denial of Service (CVE-2023-29552)

Attack Scenario: An attacker could use the SLP protocol to register arbitrary services with spoofed UDP packets, leading to an amplification attack. By sending small requests, the attacker could generate a significantly larger response, overwhelming the target system and rendering it unable to provide services to legitimate users. This denial-of-service attack could cripple key virtualization infrastructure by causing the ESXi host to crash or become unresponsive, leading to outages for all VMs hosted on the server and impacting critical business operations.

6. SSL Medium Strength Cipher Suites Supported (SWEET32)

Attack Scenario: An attacker performing a man-in-the-middle (MitM) attack on a connection between a client and the ESXi host could exploit the use of medium-strength ciphers, like those using 3DES, which are vulnerable to the SWEET32 attack. This attack involves recovering plaintext data from encrypted sessions, allowing the attacker to decrypt sensitive information (e.g., credentials or configuration data). With this decrypted information, the attacker could gain unauthorized access to the ESXi management interface or virtual machines, leading to further exploitation or data exfiltration.

PoC screenshot



7. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)

Attack Scenario: An attacker targeting a vulnerable ESXi 6.5, 6.7, or 7.0 installation could exploit one or more of the unpatched vulnerabilities in the system. This could include privilege escalation, remote code execution, or denial-of-service attacks. An attacker inside the network might leverage these vulnerabilities to take control of the host, access sensitive data, or bring down virtual machines by crashing the ESXi host. This scenario could lead to data loss, significant downtime, and a full compromise of the virtualized environment.

6. Recommendation

1. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0014) - Unsupported Version
Recommendation:

- **Upgrade** to a supported version of ESXi (preferably the latest stable version) to ensure that you continue receiving security patches and updates.
- **Regularly audit** your ESXi installations to identify unsupported versions and plan for timely upgrades.
- Implement **additional layers of security**, such as network segmentation and access controls, to reduce the risk in the interim if upgrading is delayed.

2. ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)
Recommendation:

- **Apply security patches** provided by VMware that address the XSS vulnerability.
- Ensure that only **trusted personnel** have administrative access to virtual machine properties and the ESXi Host Client.
- Use **input sanitization** techniques where applicable and restrict access to vulnerable systems until they are fully patched.
- Implement **multi-factor authentication (MFA)** to protect against session hijacking and elevate security.

3. VMware ESX / ESXi Unsupported Version Detection
Recommendation:

- **Upgrade to a supported ESXi version** that is actively maintained by VMware to receive necessary security updates.
- **Isolate outdated systems** on the network until they are upgraded, to reduce the potential attack surface.
- Ensure **compliance with internal security policies** that mandate the use of supported software versions.

4. ESXi 6.5 / 6.7 / 7.0 RCE (VMSA-2021-0002)
Recommendation:

- **Patch** the affected ESXi hosts with the latest updates to address the heap-overflow vulnerability in OpenSLP.
- If the OpenSLP service is not required, **disable the SLP service** on ESXi hosts to reduce the attack surface. Follow VMware's guidance for disabling unused services.
- Restrict access to **port 427** using network firewalls or ESXi host firewall configurations to limit exposure to unauthorized actors.

5. ESXi < 7.0 Reflected Denial of Service (CVE-2023-29552)
Recommendation:

- **Upgrade to ESXi 7.0 or later** to resolve the SLP vulnerability.
- Use **rate-limiting** or other network traffic controls to prevent abuse of SLP traffic

by attackers.
- Consider **disabling the SLP service** if it is not needed, based on your infrastructure's requirements.

6. SSL Medium Strength Cipher Suites Supported (SWEET32)
Recommendation:
- **Disable medium-strength ciphers** and **reconfigure the ESXi host** to use only strong cipher suites, ensuring that encryption uses modern algorithms (e.g., AES).
- Review SSL/TLS configurations to **enforce stronger cryptographic standards** and minimize exposure to cryptographic attacks.
- Periodically **test SSL implementations** using security tools (e.g., SSL Labs) to identify and resolve weak cipher issues.

7. ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)
Recommendation:
- **Update to the latest ESXi patch** that resolves these multiple vulnerabilities.
- Conduct **regular vulnerability scans** and ensure prompt patch management to minimize the window of exposure.
- Strengthen **access control policies** to limit administrative and remote access to the ESXi.

7. Conclusion

The assessment of the in-scope assets has uncovered a substantial exposure in the attack surface, primarily attributed to vulnerabilities stemming from inadequate configuration management. These weaknesses leave the assets at a heightened risk of exploitation, which could lead to data breaches, service disruptions, and unauthorized access. Immediate attention is required to mitigate these risks and fortify the security posture.
To enhance the security of the affected systems, the following steps are essential:

1. **Apply Security Best Practices:** Ensuring that all systems adhere to industry best practices for configuration management is crucial. This includes standardizing configurations, eliminating default settings, and enabling security features such as encryption and access control.

2. **Regular Patching and Updates:** Implementing a robust patch management process to ensure that all software and systems are regularly updated with the latest security patches will address vulnerabilities and minimize potential attack vectors.

3. **Harden Configurations:** Fine-tuning system configurations by disabling unnecessary services, restricting privileges, and enforcing the principle of least privilege (PoLP) will significantly reduce the opportunities for attackers to exploit misconfigurations.

4. **Continuous Monitoring:** Establishing continuous monitoring for configuration drift and unauthorized changes will help detect vulnerabilities in real time and maintain the integrity of the assets.

5. **Strengthen Access Controls:** Enforce multi-factor authentication (MFA) and role-based access control (RBAC) to prevent unauthorized access and limit potential damage from compromised accounts.

Cyper Space Red Team
Best Wishes