Internal / External Security Assessment Report.

PREPARED FOR

ABC Corporation.

PROJECT NAME: Q1 ABC SECURITY ASSESSMENT

Assessment Period	
Start Date	DD/MM/YYYY
End Date	DD/MM/YYYY

1 CONTENTS

1.1 Document Control

Version	Date	Author	Description
1.0	DD/MM/YYYY	Pentester / Company Name	Initial Report
1.1	DD/MM/YYYY	Pentester / Company Name	Re-assessment
1.2	DD/MM/YYYY	Pentester / Company Name	Finalized

2 EXECUTIVE SUMMARY

The security assessment conducted between the agreed upon dates was based around the scope of work detailed in the Scope of Engagement section listed below. Multiple tests were conducted against the targeted systems, involving both automated scanning and manual testing, to identify a range of potential vulnerabilities and misconfiguration of the systems.

The security team performed an internal and external security assessment for **ABC Corporation**. The assessment was performed from both authenticated and unauthenticated perspectives with the provided credentials.

Throughout the assessment, a total of **twelve** discoveries were made and documented in the report. These findings have been classified based on their impact, resulting in four **high-impact, two medium-impact, and six low-impact** vulnerabilities included in the report to enhance the overall security posture of the web application. A summary of the assessment findings is provided below.

Finding Summary

During the assessment, it was observed that the multiple hosts were missing security patches from Microsoft. Exploit code is widely available to exploit issues marked as "critical" or "important.". The Metasploit Framework is a freely available tool that provides an attacker with a point-and-click interface to launch attacks against the vulnerable server.

The affected hosts have common client software installed, which is out of date. A significant number of these hosts are therefore vulnerable to one or more of these vulnerabilities. These types of vulnerabilities in this type of software often increase the risk of phishing and spear phishing attacks, where an attacker sends an email to a user coercing them to visit a website, and once on the website, crafted attacks against the Java installation can be launched to gain internal corporate network access. As client software is out of date, this could be an indicator that the current client software patching policy requires review.

A Transport Layer Security (TLS)-protected service was found to be insufficiently protected against known cryptographic attacks. This could allow a well-positioned attacker to decrypt some or all intercepted data back to plaintext, leading to information and data theft, or it could affect the integrity of data in transit. These attacks are well known, although they require an attacker to be positioned with the ability to perform a man-in-the-middle attack, and the attacks are often non-trivial to execute.

It was possible to add a record to a zone using the DNS dynamic update protocol, as described by RFC 2136. This protocol can be used by DHCP clients to enter their host names into the DNS maps, but it could be subverted by malicious users to redirect network traffic.

The affected hosts do not require SMB signing. SMB signing is a feature that is designed to confirm the authenticity of SMB packets and prevent tampering and man-in-the-middle (MiTM) attacks. When SMB signing is not required, an unauthenticated attacker on the local area network (LAN) can exploit this weakness by modifying and relaying SMB packets between a client and a host of their choosing when the relevant other pre-requirements are in place to establish an authenticated connection.

The remote terminal services are not configured to use network-level authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

If the affected hosts are public in production, weaknesses of this nature make it more difficult for users to verify the authenticity and identity of the server. This could make it easier to carry out man-in-the-middle attacks against the affected hosts and potentially allow a positioned attacker to steal confidential data.

The response headers were identified to reveal software version information running on the host. Although this information may seem innocuous, it allows an attacker to identify the version of server-side components and therefore target further attacks against this specific software for known vulnerabilities. It is recommended that applications not disclose server and technology information in the server header by disabling the server signature.

A Transport Layer Security (TLS)-protected service was found to be insufficiently protected against known cryptographic attacks. This could allow a well-positioned attacker to decrypt some or all intercepted data back to plaintext, leading to information and data theft, or it could affect the integrity of data in transit. These attacks are well known, although they require an attacker to be positioned with the ability to perform a man-in-the-middle attack, and the attacks are often non-trivial to execute.

When a user logs out of the web application by clicking the logout button, this does not invalidate active sessions. In the event of a compromised account, the sessions would not be invalidated until they had expired, making it harder to secure an account. Additionally, old user sessions could potentially be reused between the user logging out and the session expiration, particularly when using a shared computer. All sessions should expire server-side upon a password change or when manually logging out of the application.

It is advised to ensure that the remediation advice offered within this report is implemented across the entirety of your computing infrastructure, rather than focused on specific pages or parameters. This can help mitigate any potential issues, which may still be present or introduced in the future.

3 PROJECT OVERVIEW

3.1 Scope of Engagement

The following Internal IP addresses were defined within the scope of this assessment:

Internal Infrastructure IP Address
1.1.1.1
2.2.2.2
3.3.3.3

The following external IP addresses were defined within the scope of this assessment:

External Infrastructure IP Address
4.4.4.4
5.5.5.5

3.2 Assessment Objectives

Performed security assessment to achieve the following key objectives based upon the agreed upon Scope of Work listed above:

- Perform a security assessment against the targets specified in the Scope of Engagement.
- Prioritise vulnerabilities based upon ease of exploitation, level of effort to remedy, and severity.
- Provide recommendations to improve security practice in line with industry best practice.
- Deliver a manageable and accurate report.

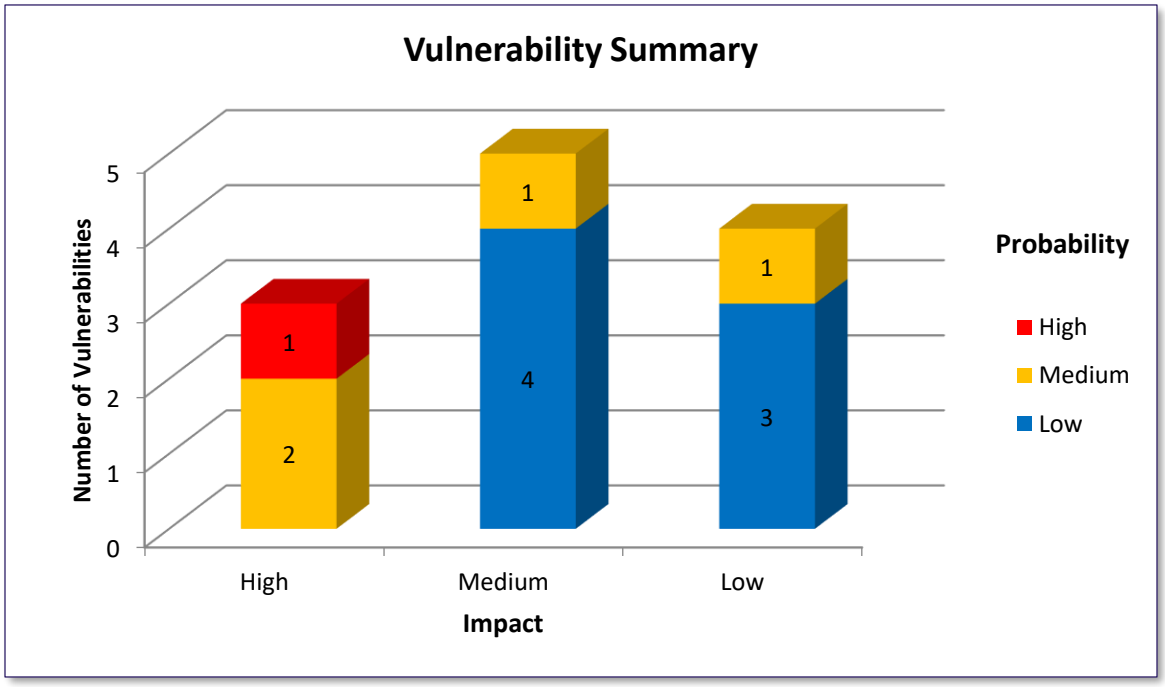
3.3 Contact Information

Contact Details	Customer Contact Details
SecureGuard Inc 123 W Madison, Suite #1700 Chicago,IL 60602 (888) 837 7776 **Tel:** **Email:** Info@ABCCorporation.com	**ABC Corporation** 1 Rhode Island Ave NE, Washington, DC 20018 (202) 555 1212 **Tel:** **Email:** Info@SecureGuardAudits.com

4 SUMMARY OF VULNERABILITIES

4.1 Graphical Summary

Key findings have been ranked and positioned in the following table according to the relative risk or probability of exploit. Vulnerabilities are split into 3 impact categories: **High**, **Medium** and **Low**. Risk is calculated by comparing the impact vs. the probability of exploit which is represented using colour coding. This was during the initial assessment.



After the retest of the application, there were no open vulnerabilities.

4.2 High Impact Vulnerabilities

The following vulnerabilities have been assigned a **High** impact rating. Successful exploitation of these vulnerabilities could lead to highly privileged access to the affected host or data or a denial-of-service condition. All the high impact vulnerabilities have been remediated and have been confirmed during the reassessment.

Risk	Description	Affected
CVSS: 9.8 **Impact/Prob: High/High**	**Amazon Linux 2 Multiple Vulnerabilities** Multiple vulnerabilities have been identified on the affected hosts, potentially leading to denial of service, information disclosure and code execution.	1.1.1.1
CVSS: 9.8 **Impact/Prob: High/High**	**Microsoft OS Patches and Service Packs: Missing Updates** The affected hosts are missing security patches and/or service packs that leave the system vulnerable to attack.	2.2.2.2.
CVSS: 8.4 **Impact/Prob: High/Medium**	**Common Client Software Outdated** The affected hosts have out-of-date client software installed that is known to contain several vulnerabilities, which may be exploited in conjunction with a phishing attack to gain access to the internal corporate network.	3.3.3.3

4.3 Medium Impact Vulnerabilities

The following vulnerabilities have been assigned a **Medium** impact rating. Exploitation of the vulnerability will not directly lead to privileged access to the host, service or data. However, vulnerabilities with a medium impact can often be combined with other flaws to elevate their impact. All the medium impact vulnerabilities have been remediated and have been confirmed during the reassessment.

Risk	Description	Affected
CVSS: 6.8 **Impact/Prob:** Medium/Medium	**Insecure TLS Configuration** The remote server has an insufficiently hardened configuration for an SSL-protected service. This means that a positioned attacker may be able to steal confidential data through a man-in-the-middle attack.	1.1.1.1
CVSS: 6.5 **Impact/Prob:** Medium/Medium	**DNS Server Dynamic Update Record Injection** It was possible to add a record into a zone using the DNS dynamic update protocol, as described by RFC 2136. This protocol can be used by DHCP clients to enter their host names into the DNS maps, but it could be subverted by malicious users to redirect network traffic	1.1.1.1
CVSS: 5.6 **Impact/Prob:** Medium/Medium	**Insecure Digital Certificate** If the affected hosts are public in production, weaknesses of this nature make it more difficult for users to verify the authenticity and identity of the server. This could make it easier to carry out man-in-the-middle attacks against the affected hosts and potentially allow a positioned attacker to steal confidential data.	1.1.1.1
CVSS: 5.3 **Impact/Prob:** Medium/Medium	**SMB Signing Not Required** The affected hosts do not require SMB Signing. SMB Signing is a feature that is designed to confirm the authenticity of SMB packets and prevent tampering and man-in-the-middle (MiTM) attacks. When SMB signing is not required an unauthenticated attacker on the Local Area Network (LAN) can exploit this weakness by modifying and relaying SMB packets between a client and a host of their choosing when the relevant other pre-requites are in place, to establish an authenticated connection.	1.1.1.1
	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	1.1.1.1

Risk	Description	Affected
CVSS: 4.0 **Impact/Prob: Medium/Low**	The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.	

5 INFRASTRUCTURE ASSESSMENT RESULT

5.1 ArubaOS-Switch - Multiple Vulnerabilities

CVSS Score: ***10.0*** ***CVSS Vector:*** *CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H* ***Impact/Probability:*** ***High/High***

CVE: *CVE-2021-25141, CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914, CVE-2019-5320, CVE-2019-5321*

Affected: *Please see the Technical Analysis section below*

Multiple vulnerabilities have been identified on the affected hosts, potentially leading to unauthorised data modification, denial of service, information disclosure and code execution.

- A security vulnerability has been identified in certain HPE and Aruba L2/L3 switch firmware. A data processing error due to improper handling of an unexpected data type in user supplied information to the switch's management interface has been identified. The data processing error could be exploited to cause a crash or reboot in the switch management interface and/or possibly the switch itself leading to local denial of service (DoS). The user must have administrator privileges to exploit this vulnerability. (CVE-2021-25141)

- The version of ArubaOS-Switch installed on the remote host is affected by multiple vulnerabilities in the Treck IP stack implementation. The vulnerabilities are collectively known as Ripple20, and can result in remote code execution, denial of service (DoS), and information disclosure by remote, unauthenticated attackers. (CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914)
  - The version of ArubaOS-Switch installed on the remote host is 16.08.* prior to version 16.08.0009, 16.09.* prior to 16.09.0007 or 16.10.* prior to 16.10.0003. It is, therefore, affected by multiple vulnerabilities, as follows:
  - A vulnerability in the Web Management Interface allows an attacker to gain access to the administration of the switch. This attack can only occur if a switch administrator is already logged into the switch Web Management Interface and is convinced by an attacker to click on the specially crafted URL. (CVE-2019-5321)
  - A vulnerability in the Web Management Interface allows an attacker to inject JavaScript code by sending a crafted URL to the administrator user of the switch. This attack can only occur if a switch administrator is already logged into the switch Web Management Interface and is convinced by an attacker to click on the specially crafted URL. (CVE-2019-5320)
  - The version of ArubaOS-Switch installed on the remote host is 16.08.* prior to version 16.08.0009, 16.09.* prior to 16.09.0007 or 16.10.* prior to 16.10.0003. It is, therefore, affected by multiple vulnerabilities, as follows:
  - A vulnerability in the Web Management Interface allows an attacker to gain access to the administration of the switch. This attack can only occur if a switch administrator is already logged into the switch Web Management Interface and is convinced by an attacker to click on the specially crafted URL. (CVE-2019-5321)
  - A vulnerability in the Web Management Interface allows an attacker to inject JavaScript code by sending a crafted URL to the administrator user of the switch. This attack can only occur if a switch administrator is already logged into the switch Web Management Interface and is convinced by an attacker to click on the specially crafted URL. (CVE-2019-5320)

5.1.1 Remediation

It is recommended to update the affected hosts to the latest possible version of the software or make any other necessary configuration changes to remediate or mitigate the issue.

5.1.2 Technical Analysis

The table below details the affected hosts:

Detail	CVE	Affected Hosts
ArubaOS-Switch Multiple Vulnerabilities (ARUBA-PSA-2020-007) Fixed release: ArubaOS-Switch 16.10.0010	CVE-2019-5320, CVE-2019-5321	1.1.1.1
ArubaOS-Switch DoS (ARUBA-PSA-2021-002) Fixed release: ArubaOS-Switch 16.10.0010	CVE-2021-25141	1.1.1.1
ArubaOS-Switch Ripple20 Multiple Vulnerabilities (ARUBA-PSA-2020-006) Fixed release: ArubaOS-Switch 16.10.0010	CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914	1.1.1.1

5.2 Microsoft OS Patches and Service Packs: Missing Updates

CVSS Score: ***9.8*** ***CVSS Vector:*** *CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H* ***Impact/Probability:*** ***High/High***

CVES: Please see the technical analysis section below.

Affected: *5.5.5.5*

Multiple hosts are missing security patches from Microsoft. Exploit code is widely available to exploit issues marked as "Critical" or "Important". The Metasploit Framework is a freely available tool that provides an attacker with a point-and-click interface to launch attacks against the vulnerable server.

Vulnerabilities marked as "Critical" by Microsoft permit remote code execution within the context of a privileged user. This would allow an attacker to gain a high level of (often administrative) control over the target server.

5.2.1 Remediation

Audit a sample of hosts and servers at regular intervals to ensure any patching policy implemented is being successfully deployed.

Windows Update Agent (WUA) is a free tool for identifying the service packs and patch level of a host or range of hosts:

https://docs.microsoft.com/en-gb/windows/win32/wua_sdk/using-wua-to-scan-for-updates-offline.

WinVerifyTrust Signature Validation

Add and enable registry value EnableCertPaddingCheck:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
```

Additionally, on 64 Bit OS systems, Add and enable the registry value EnableCertPaddingCheck:

```
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
```

5.2.2 Technical Analysis

5.2.2.1.1.1 Summary of all Missing and Misconfigured patches

The following missing patches were identified during the vulnerability scan:

SEVERITY	CVSS	CVE	PATCH	AFFECTED HOSTS
HIGH	9.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2023-50868, CVE-2024-30062, CVE-2024-30063, CVE-2024-30064, CVE-2024-30065, CVE-2024-30066, CVE-2024-30067, CVE-2024-30068, CVE-2024-30069, CVE-2024-30076, CVE-2024-30077, CVE-2024-30078, CVE-2024-30080, CVE-2024-30082, CVE-2024-30083, CVE-2024-30084, CVE-2024-30085, CVE-2024-30086, CVE-2024-30087, CVE-2024-30088, CVE-2024-30089, CVE-2024-30090, CVE-2024-30091, CVE-2024-30093, CVE-2024-30094, CVE-2024-30095, CVE-2024-30096, CVE-2024-30097, CVE-2024-30099, CVE-2024-35250	KB5039227: Windows 2022 / Azure Stack HCI 22H2 Security Update (June 2024)	5.5.5.5
HIGH	8.6 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L	CVE-2013-3900	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)	5.5.5.5
HIGH	8.8 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2023-20588, CVE-2023-21740, CVE-2023-35622, CVE-2023-35628, CVE-2023-35630, CVE-2023-35638, CVE-2023-35639, CVE-2023-35641, CVE-2023-35642, CVE-2023-35643, CVE-2023-35644, CVE-2023-36003, CVE-2023-36004, CVE-2023-36005, CVE-2023-36006, CVE-2023-36011, CVE-2023-36012, CVE-2023-36696	KB5033118: Windows 2022 / Azure Stack HCI 22H2 Security Update (December 2023)	5.5.5.5
HIGH	8.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVE-2022-35737, CVE-2024-20652, CVE-2024-20653, CVE-2024-20654, CVE-2024-20655, CVE-2024-20657, CVE-2024-20658, CVE-2024-20660, CVE-2024-20661, CVE-2024-20662, CVE-2024-20663, CVE-2024-20664, CVE-2024-20666, CVE-2024-20674, CVE-2024-20680, CVE-2024-20681, CVE-2024-20682, CVE-2024-20683,	KB5034129: Windows 2022 / Azure Stack HCI 22H2 Security Update (January 2024)	5.5.5.5

SEVERITY	CVSS	CVE	PATCH	AFFECTED HOSTS
		CVE-2024-20687, CVE-2024-20691, CVE-2024-20692, CVE-2024-20694, CVE-2024-20696, CVE-2024-20698, CVE-2024-20699, CVE-2024-20700, CVE-2024-21305, CVE-2024-21306, CVE-2024-21307, CVE-2024-21309, CVE-2024-21310, CVE-2024-21311, CVE-2024-21313, CVE-2024-21314, CVE-2024-21316, CVE-2024-21320		
HIGH	8.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVE-2023-28746, CVE-2024-21407, CVE-2024-21408, CVE-2024-21427, CVE-2024-21429, CVE-2024-21430, CVE-2024-21431, CVE-2024-21432, CVE-2024-21433, CVE-2024-21434, CVE-2024-21436, CVE-2024-21437, CVE-2024-21438, CVE-2024-21439, CVE-2024-21440, CVE-2024-21441, CVE-2024-21442, CVE-2024-21443, CVE-2024-21444, CVE-2024-21445, CVE-2024-21446, CVE-2024-21450, CVE-2024-21451, CVE-2024-26159, CVE-2024-26161, CVE-2024-26162, CVE-2024-26166, CVE-2024-26169, CVE-2024-26170, CVE-2024-26173, CVE-2024-26174, CVE-2024-26176, CVE-2024-26177, CVE-2024-26178, CVE-2024-26181, CVE-2024-26190, CVE-2024-26197	KB5035857: Windows 2022 / Azure Stack HCI 22H2 Security Update (March 2024)	5.5.5.5
HIGH	8.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVE-2024-29994, CVE-2024-29996, CVE-2024-29997, CVE-2024-29998, CVE-2024-29999, CVE-2024-30000, CVE-2024-30001, CVE-2024-30002, CVE-2024-30003, CVE-2024-30004, CVE-2024-30005, CVE-2024-30006, CVE-2024-30008, CVE-2024-30009, CVE-2024-30010, CVE-2024-30011, CVE-2024-30012, CVE-2024-30014, CVE-2024-30015, CVE-2024-30016, CVE-2024-30017, CVE-2024-30018, CVE-2024-30019, CVE-2024-30020, CVE-2024-30021, CVE-2024-30022, CVE-2024-30023, CVE-2024-30024, CVE-2024-30025, CVE-2024-30027, CVE-2024-30028, CVE-2024-30029, CVE-2024-30031,	KB5037782: Windows 2022 / Azure Stack HCI 22H2 Security Update (May 2024)	5.5.5.5

SEVERITY	CVSS	CVE	PATCH	AFFECTED HOSTS
		CVE-2024-30032, CVE-2024-30033, CVE-2024-30034, CVE-2024-30035, CVE-2024-30036, CVE-2024-30037, CVE-2024-30038, CVE-2024-30039, CVE-2024-30040, CVE-2024-30049, CVE-2024-30050, CVE-2024-30051		
HIGH	8.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVE-2023-50387, CVE-2024-20684, CVE-2024-21304, CVE-2024-21338, CVE-2024-21339, CVE-2024-21340, CVE-2024-21341, CVE-2024-21343, CVE-2024-21344, CVE-2024-21347, CVE-2024-21348, CVE-2024-21349, CVE-2024-21350, CVE-2024-21351, CVE-2024-21352, CVE-2024-21354, CVE-2024-21355, CVE-2024-21356, CVE-2024-21357, CVE-2024-21358, CVE-2024-21359, CVE-2024-21360, CVE-2024-21361, CVE-2024-21362, CVE-2024-21363, CVE-2024-21365, CVE-2024-21366, CVE-2024-21367, CVE-2024-21368, CVE-2024-21369, CVE-2024-21370, CVE-2024-21371, CVE-2024-21372, CVE-2024-21375, CVE-2024-21377, CVE-2024-21391, CVE-2024-21405, CVE-2024-21406, CVE-2024-21412, CVE-2024-21420	KB5034770: Windows 2022 / Azure Stack HCI 22H2 Security Update (February 2024)	5.5.5.5
HIGH	8.8 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	CVE-2024-20665, CVE-2024-20669, CVE-2024-20678, CVE-2024-20693, CVE-2024-21447, CVE-2024-23593, CVE-2024-23594, CVE-2024-26158, CVE-2024-26168, CVE-2024-26171, CVE-2024-26172, CVE-2024-26175, CVE-2024-26179, CVE-2024-26180, CVE-2024-26183, CVE-2024-26189, CVE-2024-26194, CVE-2024-26195, CVE-2024-26200, CVE-2024-26202, CVE-2024-26205, CVE-2024-26207, CVE-2024-26208, CVE-2024-26209, CVE-2024-26210, CVE-2024-26211, CVE-2024-26212, CVE-2024-26214, CVE-2024-26215, CVE-2024-26216, CVE-2024-26217, CVE-2024-26218, CVE-2024-26219, CVE-2024-26220, CVE-2024-26221, CVE-2024-26222,	KB5036909: Windows 2022 / Azure Stack HCI 22H2 Security Update (April 2024)	5.5.5.5

SEVERITY	CVSS	CVE	PATCH	AFFECTED HOSTS
		CVE-2024-26223, CVE-2024-26224, CVE-2024-26226, CVE-2024-26227, CVE-2024-26228, CVE-2024-26229, CVE-2024-26230, CVE-2024-26231, CVE-2024-26232, CVE-2024-26233, CVE-2024-26234, CVE-2024-26237, CVE-2024-26239, CVE-2024-26240, CVE-2024-26241, CVE-2024-26242, CVE-2024-26243, CVE-2024-26244, CVE-2024-26248, CVE-2024-26250, CVE-2024-26252, CVE-2024-26253, CVE-2024-26254, CVE-2024-26255, CVE-2024-28896, CVE-2024-28897, CVE-2024-28898, CVE-2024-28900, CVE-2024-28901, CVE-2024-28902, CVE-2024-28903, CVE-2024-28919, CVE-2024-28920, CVE-2024-28921, CVE-2024-28922, CVE-2024-28923, CVE-2024-28924, CVE-2024-28925, CVE-2024-29050, CVE-2024-29052, CVE-2024-29056, CVE-2024-29061, CVE-2024-29062, CVE-2024-29064, CVE-2024-29066, CVE-2024-29988		

5.3 Amazon Linux 2- Multiple Vulnerabilities

CVSS Score: ***9.8*** ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H* ***Impact/Probability:*** ***High/High***

CVE: *CVE-2023-20569, CVE-2023-3609, CVE-2023-3611, CVE-2023-3776, CVE-2023-20588, CVE-2023-3390, CVE-2023-34319, CVE-2023-3777, CVE-2023-39194, CVE-2023-4004, CVE-2023-4015, CVE-2023-4128, CVE-2023-4147, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-4273, CVE-2023-4622, CVE-2023-39192, CVE-2023-39193, CVE-2023-42753, CVE-2023-45871, CVE-2023-4623, CVE-2023-4921, CVE-2023-5178, CVE-2023-42755, CVE-2023-5197, CVE-2023-31085, CVE-2023-34324, CVE-2023-4244, CVE-2023-42754, CVE-2023-4881, CVE-2023-46246, CVE-2023-23583, CVE-2023-3397, CVE-2023-46813, CVE-2023-5717, CVE-2023-5752, CVE-2023-48231, CVE-2023-48232, CVE-2023-48233, CVE-2023-48234, CVE-2023-48235, CVE-2023-48236, CVE-2023-48237, CVE-2021-43618, CVE-2023-5678, CVE-2023-5678, CVE-2023-4156, CVE-2023-6277*

Affected: *1.1.1.1*

Multiple vulnerabilities have been identified on the affected hosts, potentially leading to denial of service, information disclosure and code execution.

The highest scoring CVEs are as follows:

- An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.5.3. A buffer size may not be adequate for frames larger than the MTU. (9.8, CVE-2023-45871)
- A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe-oF/TCP subsystem in the Linux kernel. This issue may allow a malicious local privileged user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation problem. (8.8, CVE-2023-5178)
- A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation.If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer. (7.8, CVE-2023-5717)
- A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. When the plug qdisc is used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect .peek handler of sch_plug and lack of error checking in agg_dequeue(). (7.8, CVE-2023-4921)
- A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploited to achieve local privilege escalation. If a class with a link-sharing curve (i.e. with the HFSC_FSC flag set) has a parent without a link-sharing curve, then init_vf() will call vttree_insert() on the parent, but vttree_remove() will be skipped in update_vf(). This leaves a dangling pointer that can cause a use-after-free. (7.8, CVE-2023-4623)
- Sequence of processor instructions leads to unexpected behavior for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege and/or information disclosure and/or denial of service via local access. (CVE-2023-23583)
- A heap out-of-bounds read flaw was found in builtin.c in the gawk package. This issue may lead to a crash and could be used to read sensitive information. (CVE-2023-4156)
- GNU Multiple Precision Arithmetic Library (GMP) through 6.2.1 has an mpz/inp_raw.c integer overflow and resultant buffer overflow via crafted input, leading to a segmentation fault on 32-bit platforms. (CVE-2021-43618)
- An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow An attacker to cause a denial of service via a craft input with size smaller than 379 KB. (CVE-2023-6277)
- Vim is an improved version of the good old UNIX editor Vi. Heap-use-after-free in memory allocated in the function `ga_grow_inner` in in the file `src/alloc.c` at line 748, which is freed in the file `src/ex_docmd.c` in the function `do_cmdline` at line 1010 and then used again in `src/cmdhist.c` at line 759. When using the `:history` command, it's possible that the provided argument overflows the accepted value. Causing an Integer Overflow and potentially later an use-after-free. This vulnerability has been patched in version 9.0.2068. (5.5, CVE-2023-46246)
- Vim is an open source command line text editor. In affected versions when shifting lines in operator pending mode and using a very large value, it may be possible to overflow the size of integer. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `6bf131888` which has been included in version 9.0.2112. Users are advised to upgrade. There are no known workarounds for this vulnerability. (4.3, CVE-2023-48237)
- Vim is an open source command line text editor. When using the z= command, the user may overflow the count with values larger than MAX_INT. Impact is low, user interaction is required and a crash may not even happen in all situations. This vulnerability has been addressed in commit `73b2d379` which has been included in release version 9.0.2111. Users are advised to upgrade. There are no known workarounds for this vulnerability. (4.3, CVE-2023-48236)
- Vim is an open source command line text editor. When parsing relative ex addresses one may unintentionally cause an overflow. Ironically this happens in the existing overflow check, because the line number becomes negative and LONG_MAX - lnum will cause the overflow. Impact is low, user interaction is required and a

crash may not even happen in all situations. This issue has been addressed in commit `060623e` which has been included in release version 9.0.2110. Users are advised to upgrade. There are no known workarounds for this vulnerability. (4.3, CVE-2023-48235)

- Vim is an open source command line text editor. When getting the count for a normal mode z command, it may overflow for large counts given. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `58f9befca1` which has been included in release version 9.0.2109. Users are advised to upgrade. There are no known workarounds for this vulnerability. (4.3, CVE-2023-48234)
- The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-5678)
- When installing a package from a Mercurial VCS URL (ie pip install hg+...) with pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the hg clone call (ie --config). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not affect users who aren't installing from Mercurial. (CVE-2023-5752)

5.3.1 Remediation

It is recommended to update the affected hosts to the latest possible version of the software or make any other necessary configuration changes to remediate or mitigate the issue.

5.3.2 Technical Analysis

The table below details the affected hosts:

DETAIL	CVE	AFFECTED HOSTS
Amazon Linux 2: kernel (ALASKERNEL-5.10-2023-043) **Installed release:** 5.10-2023-043 **Fixed Release:** Update to the latest version. (Run 'yum update kernel' to update your system.)	CVE-2023-5717, CVE-2023-5197, CVE-2023-5178, CVE-2023-4921, CVE-2023-4881, CVE-2023-46813, CVE-2023-4623, CVE-2023-4622, CVE-2023-45871, CVE-2023-42755, CVE-2023-42754, CVE-2023-42753, CVE-2023-4273, CVE-2023-4244, CVE-2023-4208, CVE-2023-4207, CVE-2023-4206, CVE-2023-4147, CVE-2023-4128, CVE-2023-4015, CVE-2023-4004, CVE-2023-39194, CVE-2023-39193, CVE-2023-39192, CVE-2023-3777, CVE-2023-3776, CVE-2023-3611, CVE-2023-3609, CVE-2023-34324, CVE-2023-34319, CVE-2023-3397, CVE-2023-3390, CVE-2023-31085, CVE-2023-20588, CVE-2023-20569	1.1.1.1
Amazon Linux 2: microcode_ctl (ALAS-2023-2341) **Installed release**: microcode_ctl-2.1-47.amzn2.2.15 **Fixed release**: microcode_ctl-2.1-47.amzn2.4.15	CVE-2023-23583	1.1.1.1
Amazon Linux 2: gawk (ALAS-2023-2357) **Installed release**: gawk-4.0.2-4.amzn2.1.2 **Fixed release**: gawk-4.0.2-4.amzn2.1.3	CVE-2023-4156	1.1.1.1
Amazon Linux 2: gmp (ALAS-2023-2369) **Installed release**: gmp-6.0.0-15.amzn2.0.2 **Fixed release**: gmp-6.0.0-15.amzn2.0.3	CVE-2021-43618	1.1.1.1
Amazon Linux 2 : libtiff (ALAS-2023-2347) **Installed release**: libtiff-4.0.3-35.amzn2.0.19 **Fixed release**: libtiff-4.0.3-35.amzn2.0.20	CVE-2023-6277	1.1.1.1

DETAIL	CVE	AFFECTED HOSTS
Amazon Linux 2: vim (ALAS-2023-2353) **Installed release:** vim-common-9.0.1882-1.amzn2.0.3 **Fixed release:** vim-common-9.0.2120-1.amzn2.0.1 **Installed release:** vim-data-9.0.1882-1.amzn2.0.3 **Fixed release:** vim-data-9.0.2120-1.amzn2.0.1 **Installed release:** vim-enhanced-9.0.1882-1.amzn2.0.3 **Fixed release:** vim-enhanced-9.0.2120-1.amzn2.0.1 **Installed release**: vim-filesystem-9.0.1882-1.amzn2.0.3 **Fixed release:** vim-filesystem-9.0.2120-1.amzn2.0.1 **Installed release:** vim-minimal-9.0.1882-1.amzn2.0.3 **Fixed release:** vim-minimal-9.0.2120-1.amzn2.0.1 **Installed release:** xxd-9.0.1882-1.amzn2.0.3 **Fixed release:** xxd-9.0.2120-1.amzn2.0.1	CVE-2023-48237, CVE-2023-48236, CVE-2023-48235, CVE-2023-48234, CVE-2023-48233, CVE-2023-48232, CVE-2023-48231, CVE-2023-46246	1.1.1.1
Amazon Linux 2: openssl (ALAS-2023-2350) Amazon Linux 2: openssl11 (ALAS-2023-2351) **Installed release**: openssl11-libs-1.1.1g-12.amzn2.0.18. **Fixed release**: openssl11-libs-1.1.1g-12.amzn2.0.19.	CVE-2023-5678, CVE-2023-3817	1.1.1.1
Amazon Linux 2 : python-pip (ALAS-2023-2349) **Installed release**: python3-pip-20.2.2-1.amzn2.0.4 **Fixed release**: python3-pip-20.2.2-1.amzn2.0.5	CVE-2023-5752	1.1.1.1

5.4 Common Client Software Outdated

CVSS Score: ***8.4*** ***CVSS Vector:*** *CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H* ***Impact/Probability:*** ***High/Medium***

CVES: CVE-2024-31497, CVE-2023-36558, CVE-2024-0057, CVE-2024-20672, CVE-2024-21404, CVE-2024-21392, CVE-2024-21409, CVE-2024-30045, CVE-2023-36042, CVE-2024-0056, CVE-2024-0057, CVE-2024-21312, CVE-2024-21409, CVE-2024-30370, CVE-2024-36052, CVE-2023-20867, CVE-2023-20900, CVE-2023-34058, CVE-2019-5522, CVE-2022-22977, CVE-2022-31693

Affected: *1.1.1.1*

The affected hosts have common client software installed which is out of date. A significant number of these hosts are therefore vulnerable to one or more vulnerabilities. These types of vulnerabilities in this type of software often increase the risk of phishing and spear phishing attacks, where an attacker sends an email to a user coercing them to visit a website and once on the website crafted attacks against the Java installation can be launched to gain internal corporate network access. As client software is out of date this could be an indicator that the current client software patching policy requires review.

5.4.1 Remediation

Consider reviewing the client-side patching policy and technical enforcement. If no such policy exists then either consider implementing a third-party patching solution that covers software such as Java and Adobe PDF Reader, or configure software of this nature to automatically update, disable the user\'s ability to disable automatic updates wherever possible, and ensure that updates are allowed on the perimeter firewall.

* Deploying Java via Active Directory: https://www.java.com/en/download/help/msi_install.xml

* Guide for Deploying Adobe Acrobat automatically: https://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/gpo.html

5.4.2 Technical Analysis

The client software installed on the affected hosts is out of date:

SEVERITY	CVSS	CVE	PATCH	AFFECTED HOSTS
HIGH	8.1 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N	CVE-2024-31497	PuTTY < 0.81 Key Recovery Attack Vulnerability	*1.1.1.1*
HIGH	9.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2023-36558, CVE-2024-0057, CVE-2024-20672, CVE-2024-21404, CVE-2024-21392, CVE-2024-21409 CVE-2024-30045	Microsoft .net Core Multiple Vulnerabilities	*1.1.1.1*
HIGH	9.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2023-36042, CVE-2024-0056, CVE-2024-0057 CVE-2024-21312, CVE-2024-21409	Microsoft .net Framework Multiple Vulnerabilities	*1.1.1.1*
Medium	4.3 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N	CVE-2024-30370, CVE-2024-36052	WinRAR < 7.00 Multiple Vulnerabilities	*1.1.1.1*
HIGH	7.5 CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	CVE-2023-20867, CVE-2023-20900, CVE-2023-34058 CVE-2019-5522, CVE-2022-22977, CVE-2022-31693	VMware Tools Multiple Vulnerabilities	*1.1.1.1*

5.5 SNMP Agent Default Community Name (public)

CVSS Score: **7.5** ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:N* ***Impact/Probability:*** ***High***/*Medium*

CVE: CVE-1999-0517

Affected: 1.1.1.1

The affected host has a vulnerability in the “SNMP Agent Default Community Name (public)” using this It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

5.5.1 Remediation

- Disable the SNMP service on the remote host if you do not use it.
- filter incoming UDP packets going to this port or change the default community string.

5.5.2 Technical Analysis

Output

```
The remote SNMP server replies to the following default community
string :

public
```

To see debug logs, please visit individual host

Port ▲	Hosts

Figure 1 - SNMP Agent Default Community Name (public).

5.6 DNS Server Dynamic Update Record Injection

CVSS Score: *6.5* ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N* ***Impact/Probability:*** *Medium/Medium*

Affected: *1.1.1.1*

It was possible to add a record into a zone using the DNS dynamic update protocol, as described by RFC 2136.

This protocol can be used by DHCP clients to enter their host names into the DNS maps, but it could be subverted by malicious users to redirect network traffic.

5.6.1 Remediation

Ignore this warning if the scanner address is in the range of IP addresses that are allowed to perform updates.

Limit addresses that are allowed to do dynamic updates (e.g., with BIND's 'allow-update' option) or implement TSIG or SIG(0).

5.6.2 Technical Analysis

5.6.2.1.1.1Host: 1.1.1.1 [port: UDP#53]

```
It was possible to register a new A record into the following zone:


ad.example.com
```

5.7 Insecure Digital Certificate

CVSS Score: *5.6* ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L* ***Impact/Probability:*** *Medium/Medium*

CVES: CVE-2004-2761, CVE-2005-4900

Affected: *5.5.5.5*

If the affected hosts are public in production, weaknesses of this nature make it more difficult for users to verify the authenticity and identity of the server. This could make it easier to carry out man-in-the-middle attacks against the affected hosts and potentially allow a positioned attacker to steal confidential data.

5.7.1 Remediation

Ensure that certificates:

- are signed by a trusted CA.
- are currently valid and have not expired or been revoked.
- are signed with the correct hostname.
- are using strong hashing algorithms and not known vulnerable ones such as MD5 or SHA1
- do not contain RSA keys less than 2048 bits.

5.7.2 Technical Analysis

5.7.2.1.1.1SSL Certificate Signed Using Weak Hashing Algorithm

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Host: Port	Host: Port	Host: Port	Host: Port
5.5.5.5:443	5.5.5.5:8080	5.5.5.5:80	5.5.5.5:22

5.7.2.1.1.2SSL Certificate with Wrong Hostname

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Host: Port	Host: Port	Host: Port
5.5.5.5:443	5.5.5.5:8080	5.5.5.5:80

5.7.2.1.1.3SSL Self-Signed Certificate

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Host: Port	Host: Port	Host: Port	Host: Port	Host: Port
5.5.5.5:443	5.5.5.5:8080	5.5.5.5:80	5.5.5.5:22	5.5.5.5:21

5.7.2.1.1.4SSL Certificate Cannot Be Trusted

The SSL certificate for this service cannot be trusted.

Host: Port	Host: Port	Host: Port	Host: Port	Host: Port
5.5.5.5:443	5.5.5.5:8080	5.5.5.5:80	5.5.5.5:22	5.5.5.5:21

5.8 Terminal Services Doesn't Use Network Level Authentication (NLA) Only

CVSS Score: *4.0* ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N* ***Impact/Probability:*** *Medium/Low*

Affected: *1.1.1.1*

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

5.8.1 Remediation

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

5.8.2 Technical Analysis

The table below details the affected hosts:

Detail	Affected Hosts
It was possible to negotiate non-NLA (Network Level Authentication) security.	1.1.1.1

5.8.2.1.1.1Example: 1.1.1.1:3389

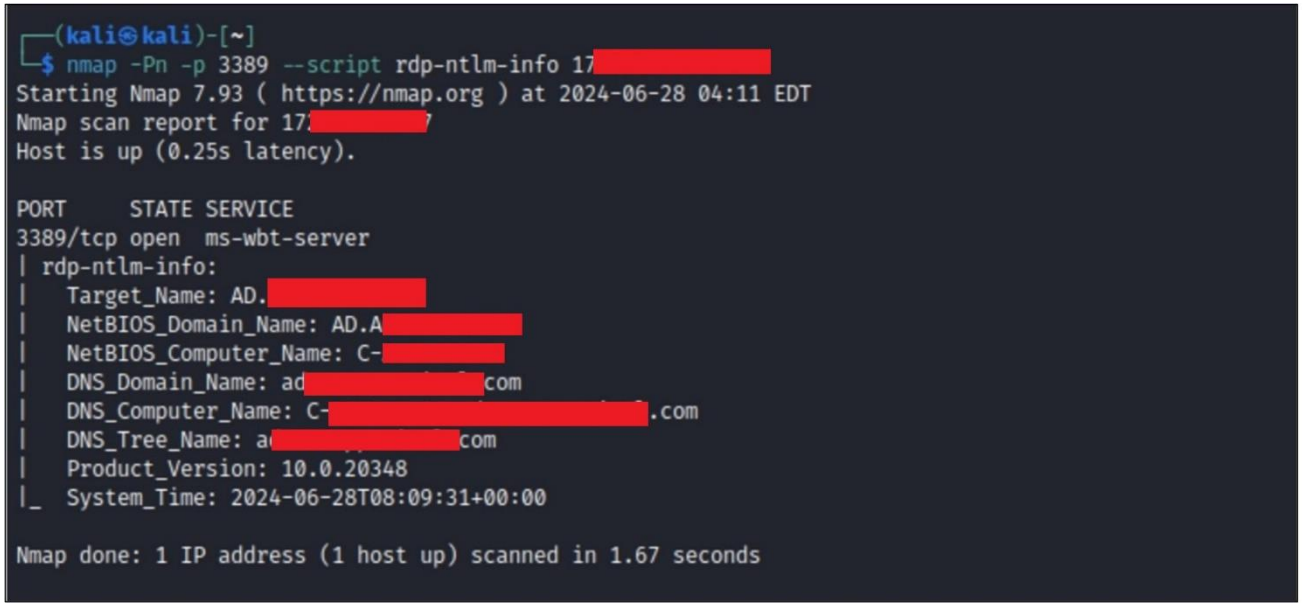


Figure 2 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only.

5.9 Information Disclosures

CVSS Score: 3.7 ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N* ***Impact/Probability: Low/Low***

Affected: 1.1.1.1,2.2.2.2

The application's HTTP response headers include version information that exposes details about the underlying software and technologies used. This disclosure can provide valuable information to potential attackers, facilitating the identification of known vulnerabilities or weaknesses associated with specific software versions.

5.9.1 Remediation

The application should be reconfigured to remove version information from HTTP headers and revealing unnecessary server-side information, thereby increasing the difficulty for an attacker to identify server configurations and reducing the possibility of an attacker exploiting publicly disclosed vulnerabilities.

5.9.2 Technical Analysis

The following table enlists disclosed server version information and by which header:

URL	HEADER	VALUE
http://1.1.1.1	Server:	Microsoft-IIS/10.0
	X-Powered-By:	ASP.NET
https://2.2.2.2	Server:	Microsoft-HTTPAPI/2.0

5.9.2.1.1.1 Example: https://1.1.1.1

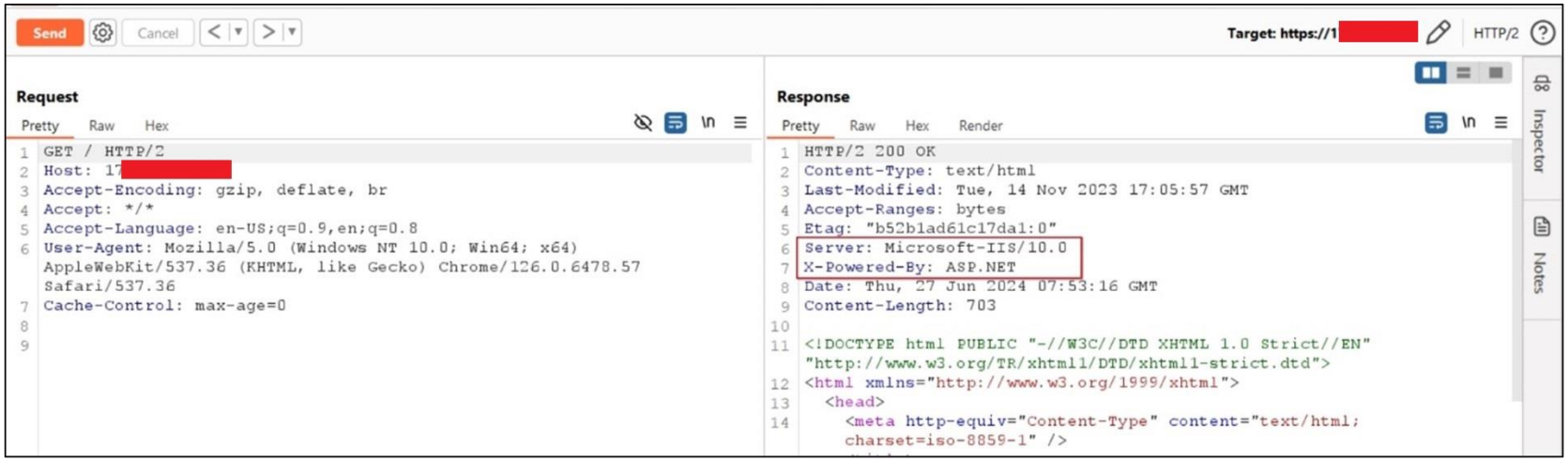


Figure 3 - Application disclosing server version information.

5.10 Microsoft IIS Default Index Page

CVSS Score: 3.7 ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N* ***Impact/Probability: Low/Low***

Affected: https://1.1.1.1

The remote web server uses the default Microsoft IIS index pages. This content can be used to fingerprint the version of the software in the technology stack of the web application or infrastructure host. As a result, a malicious actor may be able to use this information to plan further attacks.

5.10.1 Remediation

Default pages should be removed to prevent malicious users from enumerating information about the system configuration. If it is necessary to host this content, measures should be taken to ensure that it is only displayed to trusted networks and users.

5.10.2 Technical Analysis

5.10.2.1.1.1 Example: https://1.1.1.1

The following screenshot shows the default IIS welcome page was present on the mentioned host:

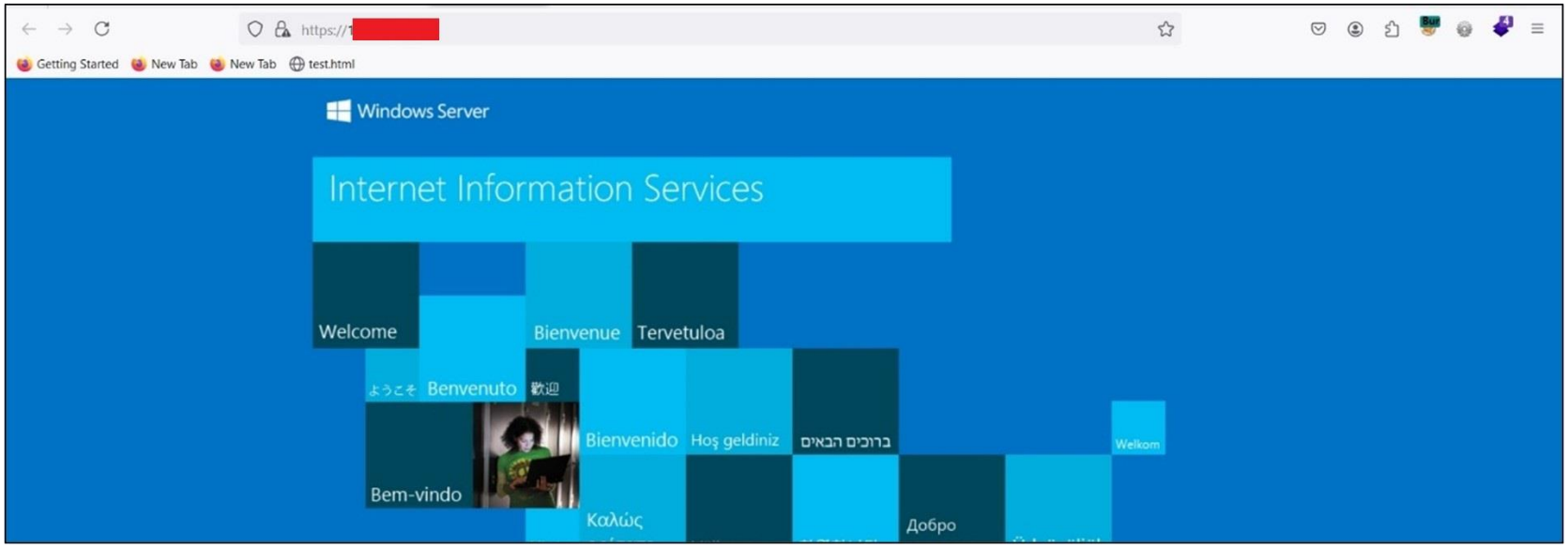


Figure 4 - Screenshot showing default IIS page in use

5.11 SSH Service Protocol/Cipher Issues

CVSS Score: 3.7 ***CVSS Vector:*** *CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N* ***Impact/Probability: Low/Low***

Affected: 1.1.1.1

The affected hosts have an SSH service which may be susceptible to cryptographic attacks which may allow an attacker to compromise communications. These attacks would require a positioned attacker with the ability to perform a man-in-the-middle attack and would be non-trivial to execute.

Common issues include SSH Protocol Version 1 Session Key Retrieval, CBC Mode Ciphers, and Weak MAC Algorithms.

5.11.1 Remediation

• Disable compatibility with version 1 of the protocol.

• Contact the vendor or consult product documentation to disable CBC mode cipher encryption and enable CTR or GCM cipher mode encryption.

• Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithm

• Contact the vendor or consult product documentation to disable arcfour algorithms

5.11.2 Technical Analysis

The table below details the affected hosts:

HOST: PORT
1.1.1.1


(kali㉿kali)-[~]
$ nmap --script ssh2-enum-algos
Starting Nmap 7.93 (https://nmap.org) at 2023-12-27 10:06 EST
Nmap scan report for ec2-3
Host is up (0.22s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
| ssh2-enum-algos:
| kex_algorithms: (12)
| server_host_key_algorithms: (5)
| ssh-rsa
| rsa-sha2-512
| rsa-sha2-256
| ecdsa-sha2-nistp256
| ssh-ed25519
| encryption_algorithms: (12)
| aes256-cbc
| blowfish-cbc
| cast128-cbc
| 3des-cbc
| mac_algorithms: (10)

6 EXTENDED INFORMATION

6.1 Port Scan

Please review the following open ports. You should ensure there are no unnecessary ports or services open.

HOST	PORT	SERVICE	VERSION
1.1.1.1	22#tcp	-	-
1.1.1.1	80#tcp	-	-
1.1.1.1	443#tcp	-	-
1.1.1.1	-	-	-
1.1.1.1	-	-	-
1.1.1.1	tcp#53	domain	Simple DNS Plus
1.1.1.1	tcp#88	kerberos-sec	Microsoft Windows Kerberos
1.1.1.1	tcp#135	msrpc	Microsoft Windows RPC
1.1.1.1	tcp#139	netbios-ssn	Microsoft Windows netbios-ssn
1.1.1.1	tcp#389	ldap	Microsoft Windows Active Directory LDAP
1.1.1.1	tcp#445	microsoft-ds	-
1.1.1.1	tcp#464	kpasswd5	-
1.1.1.1	tcp#593	ncacn_http	Microsoft Windows RPC over HTTP:1
1.1.1.1	tcp#636	ldap	Microsoft Windows Active Directory LDAP
1.1.1.1	tcp#2000	cisco-sccp	-
1.1.1.1	tcp#3268	ldap	Microsoft Windows Active Directory LDAP

HOST	PORT	SERVICE	VERSION
1.1.1.1	tcp#3269	ldap	Microsoft Windows Active Directory LDAP
1.1.1.1	tcp#3389	ms-wbt-server	Microsoft Terminal Services
1.1.1.1	tcp#5060	sip	-
1.1.1.1	tcp#53	domain	Simple DNS Plus
1.1.1.1	tcp#88	kerberos-sec	Microsoft Windows Kerberos
1.1.1.1	tcp#135	msrpc	Microsoft Windows RPC
1.1.1.1	tcp#139	netbios-ssn	Microsoft Windows netbios-ssn

7 APPENDIX A: TESTING METHODOLOGIES

The overall aim is to ensure a thorough security assessment is carried out where critical risks are identified and highlighted. Steps are taken to ensure disruption to the business is minimised and that appropriate communication paths exist to enable quick incident response. The following sections outline the methodology employed to achieve this.

7.1.1 Pre-Assessment Meeting

A pre-assessment meeting is held with the client to discuss the testing process. Testing scope is confirmed, and primary targets are identified. Any potential for disruption and data loss is discussed, critical systems are outlined and a clear incident response plan to deal with unexpected events is agreed.

7.1.2 Post-Assessment Meeting

Upon assessment completion, a meeting is held to discuss the outcomes. An overview of the findings is given with any critical and high-level vulnerabilities presented and steps to remediate these are discussed. All compromised components should be then restored to their previous state.

7.2 Internal / External Infrastructure Testing Methodology

Network Reconnaissance

Network reconnaissance is performed to identify active hosts. The network structure is mapped using DNS lookups/brute-force and zone transfers, route tracing to remote targets, extracting routing information from hosts and network devices, ping sweeps and NetBIOS nameserver enumeration.

Target Identification

At this stage, the gathered information is reviewed to find key devices that could be targeted. Thorough port scanning is conducted to identify active services on each target.

Share Enumeration

Open network shares are enumerated and examined as these may contain passwords for privileged accounts and/or sensitive data. A combination of automated tools and manual file browsing is used to achieve this.

Vulnerability Assessment

Identified services are scanned for security flaws. Typically, an unauthenticated scan is performed first to help identify vulnerabilities that can be used to gain privileged access. Once privileged access is obtained an authenticated scan may be run where additional local checks are performed to ensure more reliable results.

Vulnerability Exploitation

Security flaws discovered previously are exploited to gain access to systems and/or elevate privileges. Compromised hosts are examined for sensitive files and stored credentials that may be used to further compromise the domain. Proof of concept code is written to illustrate potential exploits.

Privilege Escalation

The overall aim is to achieve the highest level of privilege possible, (e.g. “Domain Admin” or “root”) to then gain unrestricted access to hosts connected to the domain. To assist in achieving this brute-forcing weak account passwords, password reuse, impersonation techniques and local privilege escalation exploits are used.

Data Exfiltration

Once access to sensitive data is obtained data exfiltration is verified by attempting to copy non-sensitive data residing within the internal network to an outside system controlled by the tester. This is typically done by establishing direct outbound connections, pivoting via a compromised host or re-configuring a security device.

8 APPENDIX C: VULNERABILITY RATINGS

8.1 Vulnerability Impact

Each listed vulnerability is assigned an "Impact" rating of "**High**", "**Medium**" or "**Low**". Impact is calculated by considering the potential Business Impact if the vulnerability was exploited by a malicious attacker.

Evaluation	Qualifying Factors
High	Successful exploitation could lead to highly privileged access to the target host or data. Exploitation could lead to a Denial-of-Service condition of a critical host or service.
Medium	Exploitation of the vulnerability will not directly lead to privileged access to the host, service or data. However, vulnerabilities with a medium impact can often be combined with other flaws to elevate their impact.
Low	This impact rating is assigned to vulnerabilities that, when exploited in isolation, have a negligible impact on security. Typically, vulnerabilities that disclose information that may be useful to the attacker are considered to have a low impact.

8.2 Exploitation Probability

Each listed vulnerability is assigned a "Probability" rating based upon how likely the vulnerability is to be exploited. Probability is determined by considering a number of factors including:

- How difficult the vulnerability is to exploit.
- If the vulnerability can be exploited automatically.
- If the vulnerability is or is likely to be exploited by an internet worm or botnet.
- What the attacker would achieve by exploiting the flaw.
- Probability ratings are applied subjectively whilst considering the profile of the organisation and who is likely to target the assessed resource.

The following table lists each probability evaluation rating along with a list of qualifying factors. One or more of the listed qualifying factors may be considered in each case.

Each vulnerability is evaluated on a case-by-case basis and therefore other factors that are not listed below may also be considered.

EVALUATION	QUALIFYING FACTORS
High	The vulnerability can be exploited using exploit code freely available on the internet. The vulnerability could be targeted automatically by an Internet worm or BotNet. The vulnerability could be exploited by an unskilled intruder.
Medium	To exploit the vulnerability the attacker would need to have a working knowledge of how the vulnerability operates. Some customisation to the exploit or exploit procedure is required. The attacker is required to perform a degree of social engineering to exploit the flaw and/or user interaction is required.
Low	To exploit the vulnerability the attacker would need to write custom exploit code. The vulnerability cannot be exploited reliably and/or requires in-depth knowledge of the target systems configuration. Other prerequisites must exist before the exploitation is possible and during the period of the assessment those prerequisites were not met.

8.3 Common Vulnerability Scoring System (CVSSv3)

The Common Vulnerability Scoring System version 3 (CVSSv3) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSSv3 consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment.

The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSSv3 score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Security team assigns a CVSSv3 Base score, and where necessary a CVSSv3 Temporal score, to each vulnerability where appropriate or required by various compliance standards. Vulnerabilities are often considered to have the following severity based on this scoring system:

- "**High**" severity if they have a CVSSv3 base score of 7.0 -10.0.
- "**Medium**" severity if they have a base CVSSv3 score of 4.0-6.9
- "**Low**" severity if they have a CVSSv3 base score of 0.0-3.9.