Penetration Testing Technical Report

Presented To

ABC Ltd

Oct 2022

Strictly private and confidential

V1 – October 14th, 2022

Prepared By: Benjamin Koskei

Ellan Wambugu

CONFIDENTIALITY

This document contains information, which is confidential and proprietary to. Extreme care should be exercised before distributing copies of this document, or the extracted contents of this document. XYZ is authorizing our point of contact at XYZ to view and disseminate this document as he/she sees fit in accordance with IT Policy on data handling and procedures. This document should be marked "*CONFIDENTIAL*" and therefore we suggest that this document be disseminated on a "need to know" basis.

Address questions regarding the proper and legitimate use of this document to:

Legal counsel email

DISCLAIMERS

The information presented in this document is provided as is and without warranty. Vulnerability assessments are a "point in time" analysis and as such, it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems and network.

1. Contents

2. PURPOSE

XYZ LTD has asked ABC LTD to perform a detailed security examination of their Network. This Network was their topology provided from their Headquarters where the Penetration testing would be conducted

This testing effort took place on 3rd October 022 and concluded on February 7th 2022. Some preliminary findings were provided under separate cover, and this report is being presented to show the full results of our testing efforts and to make recommendations where appropriate

3. SCOPE

The scope of this review was limited to the XYZ Network Infrastructure. This infrastructure sits on an MPLS setup where it supports3 branches distributed across the country. The Network host the centrality of IT operations in the company and the branches connected via VPN. The Scope would also include their endpoints which include Workstations, servers (Domain Controller, File Server, and Application servers) hosted on-prem, and a WIFI network.

The IP Range for the XYZ x.x.x.x /24 with Public IP: x.x.x.x/30.

4. METHODOLOGY

To conduct this test, a globally accepted industry standard framework has been used. The framework based on Penetration Testing Execution Standard (PTES) is used which outlines the following phases.

This is a 7-phased methodology: Pre-engagement gatherings, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting.

5. DISCOVERED VULNERABILITIES AND REMEDIATION STEPS

5.1 Critical Vulnerabilities

5.1.1 Microsoft SQL Server Obsolete Version.

Description:

An obsolete version of the Microsoft SQL database server is running. MySQL server 2014 12.0.4522 was found to be running on whose update release date is 2017-August. This version is susceptible to Microsoft SQL Server Remote Code Execution Vulnerability. Remote code execution (RCE) attacks allow an attacker to remotely execute malicious code on a computer. The impact of an RCE vulnerability can range from malware execution to an attacker gaining full control over a compromised machine.

Affected Nodes:

192.168.16.11 – SAP HANA server.

Vulnerability solution:

Download and apply for an upgrade. Option 1 is to Update to MYSQL 2014 version 12.0.6024.0 – Service Pack 3 or option 2 is: Upgrade to MySQL server 2019.

5.1.2 HP iLO: CVE-2018-7078: Remote or Local Code Execution (hp-ilo-cve-2018-7078)

Description:

A remote code execution was identified in HPE Integrated Lights-Out 4 (iLO 4) earlier than version v2.60 and HPE Integrated Lights Out 5 (iLO 5) earlier than version v1.30.

A security vulnerability in HPE Integrated Lights-Out 4 could be remotely or locally exploited by an administrative user to allow remote or local code execution.

Affected Nodes:

192.168.16.200 – HPE iLO

References

CVE-2018-7078

Vulnerability solution:

Upgrade HP iLO 4 to version 2.60 from https://hpe.com/support/ilo4
And Upgrade HP iLO 5 to version 1.30 from https://hpe.com/support/ilo5

5.1.3 HP iLO: CVE-2018-7105: Remote Execution of Arbitrary Code, Local Disclosure of Sensitive Information (hp-ilocve-2018-7105)

Description:

A security vulnerability in HPE iLO 5 for HPE Gen10 Servers prior to v1.35, HPE (iLO 4) prior to v2.61, and HPE iLO 5 prior to v1.90 could be remotely exploited to execute arbitrary code leading to the disclosure of information.

Affected Nodes:

192.168.16.200 – HPE iLO

Vulnerability solution:

Upgrade HP iLO 4 to version 2.61 https://hpe.com/support/ilo4

5.1.4 HP iLO: CVE-2020-11896: Code Execution, Denial of Service (hp-ilo-cve-2020-11896)

Description:

The Treck TCP/IP stack before 6.0.1.66 allows Remote Code Execution, related to IPv4 tunneling.

Affected Nodes

192.168.16.200 – HPE iLO

Reference

CVE-2020-11896 - https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf04012en_us

Vulnerability solution:

Upgrade HP iLO 4 to version 2.61

5.1.5 MMicrosoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability (msft-cve-2017-0146)

Description:

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server. To exploit the vulnerability, in most situations, an authenticated attacker could send a specially crafted packet to a targeted SMBv1 server. The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

Affected Nodes:	Additional Information:
192.168.16.55 – Domain Controller – (AD)	Host returned an expected exception that indicates vulnerability (INSUFF_SERVER_RESOURCES).

Vulnerability solution:

Cumulative Update for Windows Server 2016 for x64-based Systems (KB4013429)

Download and apply the patch from: http://support.microsoft.com/kb/4013429

5.1.6 VNC remote control service installed (backdoor-vnc-0001)

Description:

AT&T Virtual Network Computing (VNC) provides remote users with access to the system it is installed on. If this service is compromised, the user can gain complete control of the system.

Affected Nodes:	Additional Information:
192.168.16.51:5900 (MAC Address: AC:1F:6B:B8:66:16)	Vulnerable OS: AXIS 210A or 211 Network Camera (Linux 2.6.17) Running VNC service

Vulnerability Solution:

Remove or disable this service. If it is necessary, be sure to use well thought out (hard to crack) passwords. It is important to note that VNC provides additional information on available strong password mechanisms when authenticating.

To protect data from eavesdroppers, tunnelling VNC through SSH is recommended.

Additionally, restricting access to specific IP addresses using TCP wrappers is also recommended.

For more information on VNC, visit the VNC website or General Docs, or FAQ.

5.1.7 HP iLO: CVE-2018-7093: Denial of Service (hp-ilo-cve-2018-7093)

Description:

A security vulnerability in HPE Integrated Lights-Out, iLO 4 prior to v2.60, could be remotely exploited to create a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.200	Vulnerable OS: HP iLO 4The property "firmware.version" contains: 2.55.

References:

Source	Reference
CVE	CVE-2018-7093
URL	https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-hpesbhf03835en_us

Vulnerability Solution:

Upgrade HP iLO 4 to version 2.60 from https://hpe.com/support/ilo4

5.1.8 SNMP credentials transmitted in cleartext (snmp-cleartext-credential)

Description:

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings.

Affected Nodes:

Affected Nodes:	Additional Information:

192.168.16.54:161 (MAC ADDR: C4:65:16:11:52:5A)	Successfully authenticated to the SNMP v1/v2c service.

Vulnerability Solution:

1. If you do not absolutely need SNMP, disable it. SNMP versions 1 and 2c are inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP, be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

5.2 Severe Vulnerabilities

5.2.1 X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description:

The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, or else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, which should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted. Please note that this check may flag a false positive against servers that are properly configured using SNI.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.11:8100 (SAP Server)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN Administrator does not match target name specified in the site. Subject CN Administrator could not be resolved to an IP address via DNS lookup
192.168.16.12:50000 (Mac Addr: D4:F5:EF:01:D3:71, Hostname: Kagwesap.carbacid.local)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN hanabone does not match target name specified in the site. Subject CN hanabone could not be resolved to an IP
192.168.16.12:60000 (Mac Addr: D4:F5:EF:01:D3:71, Hostname: Kagwesap.carbacid.local)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN hanabone does not match target name specified in the site. Subject CN hanabone could not be resolved to an IP address via DNS lookup Subject Alternative Name hanabone does not match target name specified in the site. Subject Alternative Name 16.1.15.2 does not match target name specified in the site.

192.168.16.123:8444 (Mac Addrr: 94:18:82:0B:B2:B1)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN www.adauditplus.com does not match target name specified in the site. Subject CN resolved IP address differs from node IP address specified in the site. Subject CN resolved IP address differs from node IP address specified in the site.
192.168.16.181:8443 (Mac Addr: 00:15:5D:10:0A:1F)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN entrust-intellitrust-agent does not match target name specified in the site. Subject CN entrust-intellitrust-agent could not be resolved to an IP address via DNS lookup
192.168.16.200:443 (iLO HPE)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN ILOCZJ64107W8 does not match target name specified in the site. Subject CN ILOCZJ64107W8 could not be resolved to an IP address via DNS lookup Subject Alternative Name ILOCZJ64107W8 does not match target name specified in the site.
192.168.16.51:443 (Mac Addr: AC:1F:6B:B8:66:16)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN IPMI does not match target name specified in the site. Subject CN IPMI could not be resolved to an IP address via DNS lookup
192.168.16.57:443 (Mac Addr: AC:1F:6B:B4:B9:F1)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN backup. Local does not match target name specified in the site. Subject CN backup. Local could not be resolved to an IP address via DNS lookup

192.168.16.64:8443 (Mac Addr: 48:D6:D5:3E:85:F4)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN 3L09HY FA8FCA888704 does not match target name specified in the site. Subject CN 3L09HY FA8FCA888704 could not be resolved to an IP address via DNS lookup
192.168.16.76:8443 (Macc Addr: 3C:D9:2B:0B:73:32)	The subject common name found in the X.509 certificate does not seem to match the scan target: Subject CN SERVER1 does not match target name specified in the site. Subject CN resolved IP address differs from node IP address specified in the site.

Vulnerability Solution:

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

5.2.2 CIFS Account Password Never Expires (cifs-acct-password-never-expires)

Description:

The CIFS account does not require password expiration. This is a security risk. Having no password expiration allows a hacker to launch a brute force attack to guess the user's password. This can be done with greater success over a prolonged period of time if the password never expires.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.12 (Hostname: Kagwesap.carbacid.local)	Password does not expire: b1techuser
192.168.16.12 (Kagwesap.carbacid.local)	Password does not expire: b1scswworkingshare

Vulnerability Solution:

If the account is not used, delete or disable the account. If the account is a built-in system account such as the IUSR_ or IWAM_ accounts, enable the "User cannot change password" option to stop this vulnerability from being reported (Microsoft best practices dictate that built-in system accounts NOT be allowed to change their own passwords). Otherwise, ensure that the password expires by disabling the "Password never expires" option.

1. Right click on "My Computer"
2. Select "Manage"
3. Open the "Local Users and Groups" folder
4. Open the "Users" folder
5. Double-click on the desired user
6. Uncheck "Password never expires"

5.2.3 SMB signing disabled (cifs-smb-signing-disabled)

Description:

This system does not allow SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.11:139	SMB signing is disabled
192.168.16.11:445	SMB signing is disabled
192.168.16.117:139	SMB signing is disabled
192.168.16.117:445	SMB signing is disabled
192.168.16.121:139	SMB signing is disabled
192.168.16.121:445	SMB signing is disabled
192.168.16.126:139	SMB signing is disabled
192.168.16.126:445	SMB signing is disabled
192.168.16.134:139	SMB signing is disabled
192.168.16.134:445	SMB signing is disabled
192.168.16.196:139	SMB signing is disabled
192.168.16.196:445	SMB signing is disabled

References:

Source	Reference
URL	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-

Source	Reference
	smb2.aspx

Vulnerability Solution:

Configure SMB signing for Windows.Configure the system to enable or require SMB signing as appropriate. The method and effect of doing this is system specific so please see this Microsoft article for details. Note: ensure that SMB signin configuration is done for incoming connections (Server).

5.2.4 IPMI 2.0 RAKP RMCP+ Authentication HMAC Password Hash Exposure (ipmi2-rmcp-rakp-hmac-password-hashexposure)

Description:

The IPMI 2.0 specification supports HMAC-SHA1 and HMAC-MD5 authentication, both of which send a computed hash to the client that can be used to mount an offline brute force attack of the configured password.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.200:623	Successfully negotiated IPMI RMCP+ open session request with cipher type 1
192.168.16.51:623	Successfully negotiated IPMI RMCP+ open session request with cipher type 1

References:

Source	Reference
URL	https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi

Vulnerability Solution:

i. Disable IPMI entirely using the links below or by consulting your vendor's documentation: SuperMicro IPMI User Guide

ii. Restrict access the affected IPMI service(s) using a firewall or other appropriate technology

5.2.5 SMB: Service supports deprecated SMBv1 protocol (cifs-smb1-deprecated)

Description:

The SMB1 protocol has been deprecated since 2014 and is considered obsolete and insecure.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.11:139	SMB1 is deprecated and should not be used
192.168.16.11:445	SMB1 is deprecated and should not be used
192.168.16.117:139	SMB1 is deprecated and should not be used
192.168.16.117:445	SMB1 is deprecated and should not be used
192.168.16.121:139	SMB1 is deprecated and should not be used
192.168.16.121:445	SMB1 is deprecated and should not be used
192.168.16.123:139	SMB1 is deprecated and should not be used
192.168.16.123:445	SMB1 is deprecated and should not be used
192.168.16.126:139	SMB1 is deprecated and should not be used
192.168.16.126:445	SMB1 is deprecated and should not be used
192.168.16.134:139	SMB1 is deprecated and should not be used
192.168.16.134:445	SMB1 is deprecated and should not be used

192.168.16.196:139	SMB1 is deprecated and should not be used
192.168.16.196:445	SMB1 is deprecated and should not be used
192.168.16.55:139	SMB1 is deprecated and should not be used
192.168.16.55:445	SMB1 is deprecated and should not be used

References:

Source	Reference
URL	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

Vulnerability Solution:

Windows Server 2012 R2, removing SMB1 is trivial. On older OS'es it can't be removed but should be disabled. This article contains system-specific details:

How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server

5.2.6 Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.6 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.11:1433 (AD)	Running TDS service
192.168.16.76:1433 (Server 1, Mac Addr: 3C:D9:2B:0B:73:32)	Running TDS service

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

5.2.7 Microsoft IIS default installation/welcome page installed (http-iis-default-install-page)

Description:

The IIS default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, IIS is installed by default and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.11:81 (SAP Server)	Running HTTP service Product IIS exists -- Microsoft IISHTTP GET request to http://192.168.16.11:81/
192.168.16.123:81 (Mac Addr: 94:18:82:0B:B2:B1, hostname: Carbacid:)	Running HTTP service Product IIS exists -- Microsoft IISHTTP GET request to http://192.168.16.123:81/
192.168.16.196:80 (Hostname: Cylinder)	Running HTTP service Product IIS exists -- Microsoft IISHTTP GET request to http://192.168.16.196/
192.168.16.76:80 (Server 1)	Running HTTP service Product IIS exists -- Microsoft IISHTTP GET request to http://192.168.16.76/

Vulnerability Solution:

If this server is required to provide necessary functionality, then the default page should be replaced with relevant content. Otherwise, this server should be removed from the network, following the security principle of minimum complexity.

If the server is not needed, it can be disabled in the following way: in the Services window of the Control Panel's Administrative Tools section, right-click on the 'World Wide Web Server' entry and select 'Stop'. Set its startup type to 'Manual' so that it does not restart if the machine is rebooted (this is done by selecting 'Properties' in the right-click menu).

5.2.8 SSH Birthday attacks on 64-bit block ciphers (SWEET32) (ssh-cve-2016-2183-sweet32)

Description:

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. The security of a block cipher is often reduced to the key size k: the best attack should be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an important security parameter, defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than 2 to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.200:22	Running SSH service Insecure 3DES ciphers in use: 3des-cbc

References:

Source	Reference
CVE	CVE-2016-2183

URL	https://sweet32.info/

Vulnerability Solution:

Remove all 3DES ciphers from the cipher list specified in sshd_config.

5.2.9 TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) (ssl-cve-2016-2183-sweet32)

Description:

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of the SSL/TLS protocols that support cipher suites which use 3DES as the symmetric encryption cipher are affected. The security of a block cipher is often reduced to the key size k: the best attack should be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an important security parameter, defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than 2 to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.11:3389 (SAP Server)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers:

	TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.116:3389 (Server1)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.117:3389 (Gabriel)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.121:3389 (Angelak)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.123:443 (Carbacid)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA

192.168.16.123:636 (Carbacid)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.123:3269 (Carbacid)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.123:3389 (Carbacid)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
Affected Nodes:	Additional Information:
192.168.16.126:3389 (lauransa1)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA

192.168.16.134:3389 (johnk)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.196:3389 (cylinder)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.200:443 (iLO HPE)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
192.168.16.76:3389 (Server 1)	Negotiated with the following insecure cipher suites: TLS 1.0 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.1 ciphers:

	TLS_RSA_WITH_3DES_EDE_CBC_SHATLS 1.2 ciphers: TLS_RSA_WITH_3DES_EDE_CBC_SHA

References:

Source	Reference
CVE	CVE-2016-2183
URL	https://sweet32.info/
URL	https://www.openssl.org/blog/blog/2016/08/24/sweet32
URL	https://access.redhat.com/articles/2548661

Vulnerability Solution:

Configure the server to disable support for 3DES suite.

5.2.10 Self-signed TLS/SSL certificate (ssl-self-signed-certificate)

Description:

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL manin-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.11:8100	TLS/SSL certificate is self-signed.
192.168.16.12:50000	TLS/SSL certificate is self-signed.
192.168.16.12:60000	TLS/SSL certificate is self-signed.
192.168.16.123:443	TLS/SSL certificate is self-signed.
192.168.16.123:2381	TLS/SSL certificate is self-signed.
192.168.16.123:3389	TLS/SSL certificate is self-signed.
192.168.16.123:8444	TLS/SSL certificate is self-signed.
192.168.16.181:8443	TLS/SSL certificate is self-signed.
192.168.16.196:3389	TLS/SSL certificate is self-signed.
192.168.16.51:443	TLS/SSL certificate is self-signed.
192.168.16.57:443	TLS/SSL certificate is self-signed.
192.168.16.76:8443	TLS/SSL certificate is self-signed.

Vulnerability Solution:

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or Verisign.

5.3 Moderate Vulnerabilities

5.3.1 SSH CBC vulnerability (ssh-cbc-ciphers)

Description:

SSH contains a vulnerability in the way certain types of errors are handled. Attacks leveraging this vulnerability would lead to the loss of the SSH session. According to CPNI Vulnerability Advisory SSH:
If exploited, this attack can potentially allow an attacker to recover up to 32 bits of plaintext from an arbitrary block of ciphertext from a connection secured using the SSH protocol in the standard configuration.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.16.200:22	Running SSH serviceInsecure CBC ciphers in use: aes256-cbc,aes128cbc,3des-cbc
192.168.16.57:22	Running SSH serviceInsecure CBC ciphers in use: aes256-cbc,aes128-cbc

References:

Source	Reference
URL	https://www.kb.cert.org/vuls/id/958563

Vulnerability Solution:

SSH can be done using Counter (CTR) mode encryption. This mode generates the keystream by encrypting successive values of a "counter" function. In order to mitigate this vulnerability SSH can be setup to use CTR mode rather CBC mode

6.0 Conclusion

The vulnerabilities classified as critical need to be fixed immediately followed subsequently by the classified as Severe.

-END-