Vulnerability Assessment & Penetration Testing

November 2017

Srinjoy Chakravarty

Glossary

What are do the different recommendation levels mean?

The following is a generalized estimation and may not reflect ground realities of implementing a proposed solution at J**** / S*******.

Recommendation	Description
Interim Action	Priority action to patch significant vulnerability and prevent hack Often involves enabling a configuration available on existing infrastructure Time: 1–7 Days Implementation Cost: Negligible
Short Term Solution	Good practice generally implemented by companies in a similar environment Often involves addition modules to existing infrastructure Time: 1–2 Weeks Implementation Cost: Economical
Medium Term Setup	Supplements initial patch and protects against a majority of attack vectors Time: 2–4 Weeks Implementation Cost: Reasonable
Long Term Implementation (Optimum)	Requires dedicated resources, hardware acquisition and implementation team Time: 1-2 Months to Plan/Choose Vendor & 3-4 Month Engagement to Deploy Implementation Cost: Significantly High (Requires Dedicated Budget)
Long Term Implementation (Most Secure)	An optional state-of-the-art solution that can be chosen as an alternative to the optimum implementation Time: 3-4 Months to plan/tender & 5-6 Months Engagement to Deploy Implementation Cost: Very Expensive (Requires Special Business Justification)

What are Recommendations labeled with numbers and alphabets?

Numbering indicates a recommended chronology of remedial actions

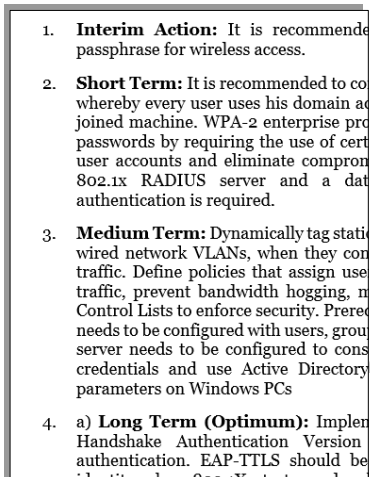
Week 1

Week 4

Week 7

Alphabetization within a specific number indicates a decision point where one of the proposed implementations may be pursued

Option A (Week 10)



1. **Interim Action:** It is recommende passphrase for wireless access.
2. **Short Term:** It is recommended to co whereby every user uses his domain ac joined machine. WPA-2 enterprise pro passwords by requiring the use of cert user accounts and eliminate compron 802.1x RADIUS server and a dat authentication is required.
3. **Medium Term:** Dynamically tag stati wired network VLANs, when they con traffic. Define policies that assign use traffic, prevent bandwidth hogging, n Control Lists to enforce security. Prerec needs to be configured with users, grou server needs to be configured to cons credentials and use Active Directory parameters on Windows PCs
4. a) **Long Term (Optimum):** Implen Handshake Authentication Version authentication. EAP-TTLS should be

b) **Long Term (Most Secure):** In
certificate authentication between cli

What does the CVSS score mean?

Severity Level	CVSS Score	Guidance
Critical	9.1 - 10.0	A vulnerability whose exploitation could allow system compromise and malware propagation without any user interaction and whose exploits are in the wild
High	7.0 – 9.0	A vulnerability whose exploitation could result in compromise of the confidentiality or integrity of user data or availability of processing resources, but which requires some degree of user interaction
Medium	4.1 - 6.9	A vulnerability that could cause privilege escalation or sensitive data exposure but which is mitigated to a significant degree by factors such as default configuration or auditing
Low	0.1 – 4.0	A vulnerability whose exploitation is extremely difficult or whose impact is minimal and may only cause non-sensitive data exposure

How are CVSS scores calculated?

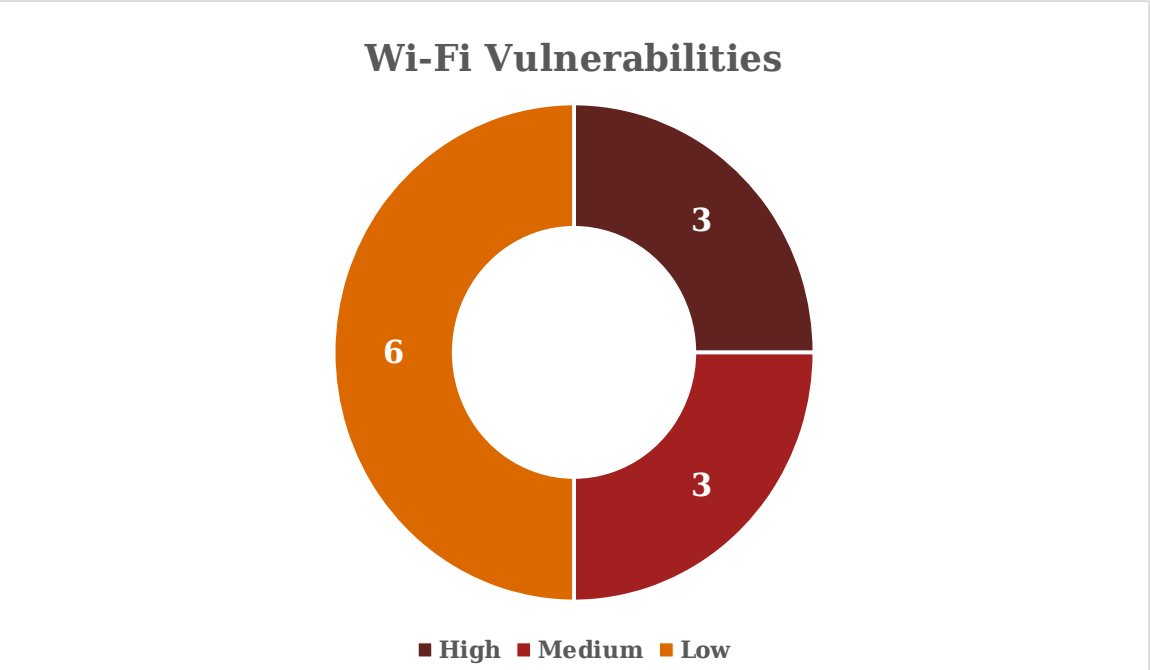
$$Exploitability = 20 \times AccessVector \times AccessComplexity \times Authentication$$

$$Impact = 10.41 \times (1 - (1 - ConfImpact) \times (1 - IntegImpact) \times (1 - AvailImpact))$$

$$f(Impact) = \begin{cases} 0, & \text{if } Impact = 0 \\ 1.176, & \text{otherwise} \end{cases}$$

$$BaseScore = roundTo1Decimal(((0.6 \times Impact) + (0.4 \times Exploitability) - 1.5) \times f(Impact))$$

1. Wireless Security Assessment



Wireless Networks (SSIDs) Tested

1. *S*******
2. *S*******-6
3. STC_Corporate
4. STC_Guest
5. JW-CC-TECH

1.1 Wi-Fi Passphrase Vulnerable to Dictionary-Based At

Score:

Description

The S******* network is vulnerable to attackers as they can compromise the network by cracking the WPA2 Wireless key or enumerating the key from a machine which is not authenticated to the wireless network. With access to the network, the attacker may even sniff the traffic and redirect users to malicious website. The S******* Wi-Fi network has a weak password which can be acquired by capturing the hash from WPA2's four-way handshake.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	Low
Temporal Score	
Exploit maturity	Functional
Remediation level	Official-Fix
Report confidence	Confirmed

Impact

Once the four-way handshake of the S******* Wi-Fi network is captured, a dictionary based attack against the hashes was conducted to crack the password hash. In cases where the password is more complex, the attacker would harvest the packet capture offline and lease supercomputer resources on the cloud to crack the hash. Moreover, simple shoulder surfing allows a malicious onlooker from finding out the wireless network password.

Affected Targets

S*******

Recommendation

1. **Interim Action:** It is recommended to configure a strong, complex WPA-2 passphrase for wireless access.
2. **Short Term:** It is recommended to configure the networks to use WPA2-enterprise whereby every user uses his domain account to access the network using a domain joined machine. WPA-2 enterprise provides an insurance policy against weak user passwords by requiring the use of certificates and allows administrators to disable user accounts and eliminate compromised machines. Prerequisite: To do this an 802.1x RADIUS server and a database of separate client credentials for authentication is required.
3. **Medium Term:** Dynamically tag stations based on user or group identity in existing wired network VLANs, when they connect over the wireless network to segregate traffic. Define policies that assign users to different VLANs that prioritize critical traffic, prevent bandwidth hogging, manage network bottlenecks and use Access Control Lists to enforce security. Prerequisite: To do this, the 802.1x RADIUS server needs to be configured with users, groups and VLAN tags. Prerequisite: The RADIUS server needs to be configured to consult with a Domain Controller to verify user credentials and use Active Directory Group Policy Objects to manage 802.1X parameters on Windows PCs
4. a) **Long Term (Optimum):** Implement EAP-TTLS with Microsoft's Challenge-Handshake Authentication Version 2 which provide server-side certificate authentication. EAP-TTLS should be configured to send an anonymous client identity when 802.1X starts, and only send the actual client identity once the Transport Layer Security tunnel has been established.

   b) **Long Term (Most Secure):** Implement EAP-TLS which provides mutual certificate authentication between client and server, using the Transport Layer Security protocol. Prerequisite: To do this, clients will require digital certificates and require them to be managed by a Public Key Infrastructure.

Screenshot

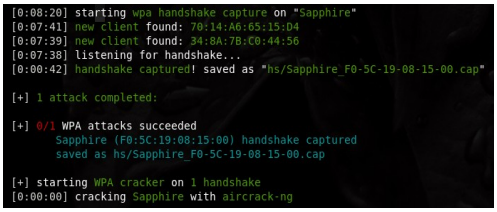


Figure 1: Four-way WPA Handshake captured when a user's device

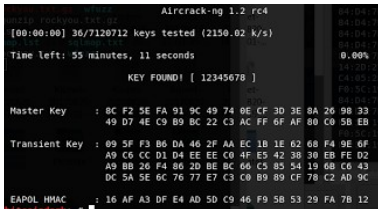


Figure 2: Key cracked in under 9 minutes when with default wordlist with an 8GB

Figure 1 Figure 2

References

https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified/

http://searchnetworking.techtarget.com/feature/Combini authorization?track=wsl3

Critica **Hig** Medium Low Info

http://searchnetworking.techtarget.com/feature/Choosing-the-right-flavor-of-8021X

1.2 Unrestricted Access Control Bypass via Guest Wi-Fi

Score:

Description

The STC_Guest network is vulnerable to access control bypass. An attacker can sniff wireless traffic on the STC_Guest network and list MAC addresses of connected clients. They can then connect their machine to the open Guest Wi-Fi and bypass the web login access control by spoofing any of the connected MAC addresses and gain access to the internet to conduct malicious activity without being identified.

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	None
Temporal Score	
Exploit maturity	High
Remediation level	Official Fix
Report confidence	Confirmed

Affected Targets
STC_Guest

Impact

Wireless networking, more than any other networking technology needs authentication and an access control mechanism as attackers tend to look for open wireless networks to conduct malicious acts on other users and networks. MAC spoofing defeats the principle of non-repudiation as all malicious activity conducted by the attacker will be falsely attributed to their victim. Attacks conducted on the internet may create reputational damage for J**** as the malicious network traffic will be rooting from J****'s networks.

Recommendation

1. **Interim Action:** Ensure guest network is completely segregated from other corporate networks
2. **Short Term:** Configure rule on the wireless controller to leverage the conflict attribute which checks for device conflicts and trips if the device category changes.
3. **Medium Term:** Configure the web authentication to a strict one MAC address per user login, with a session timeout value that forces re-authentication after an idle time out value has been surpassed.
4. **Long Term:** Implement detection of masqueraded wireless access using 802.11 MAC-layer fingerprints

Screenshot

Figure 1: Shows the MAC address of a legitimate user connected to STC_Guest spoofed to successfully gain

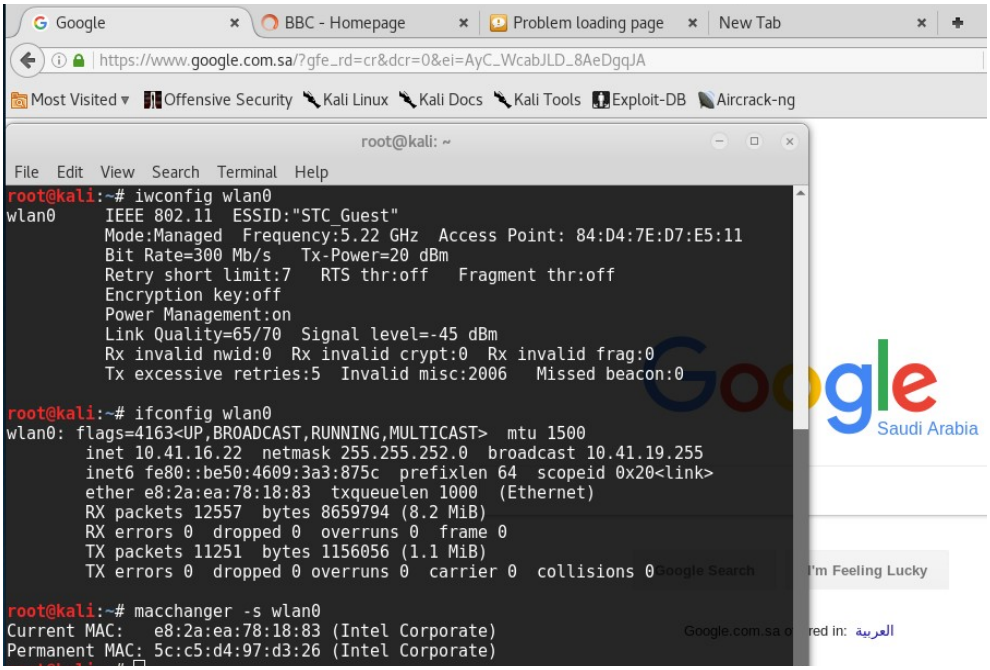


Figure 1

References

http://community.arubanetworks.com/t5/Security/MAC-spoofing-and-clear-pass-mac-authentication/td-p/260814

http://community.arubanetworks.com/t5/Security/Device-connect/td-p/20

https://tradlosetrondheim.no/pdf/Spoof_WiFi.pdf

Critica Hig Medium Low Info

1.3 Weak Fingerprint Scanner Security

Score:

Description

The S******* fingerprint access point can be accessed by unauthorized users both from the Wi-Fi network and externally from the Suprema endpoint device. We found that the Suprema biometric device is reachable (through ping) once a user is connected to S******* network which has a relatively generic network key. Additionally, the admin console of the biometric device can be accessed physically which does not have an admin password. This is even more alarming when coupled with the CCTV access gained as displayed in the subsequent findings.

Environmental Score	
Attack vector	Physical
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	Low
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Not defined
Remediation level	Temporary fix
Report confidence	Confirmed

Affected Targets
Supreme Biometric

Impact

A potential attacker can gain access to J**** premises without detection by using the elevators to reach the 34th floor without authentication after normal office hours. They can then tamper with the fingerprint console to gain administrative privileges on the system, exfiltrate the configuration details of Suprema's Access Control setup including the network and database configuration via USB. Once harvested, the attacker can perform a custom install of the Biostar administrative console on their machine and connect to the existing database, gaining access to Personally Identifiable Information of all the registered employees in the process. From there, the attacker can purge the entire database to lock out employees from J****'s premises, give themselves physical access to office premises to engage in further malicious activity (asset theft, network infiltration, power supply trip etc.) and escalate privileges to retain full control of the Suprema biometric system.

Recommendation

Figure 1: Shows that the fingerprint device is accessible across

1. **Interim Action:** Change the default master password and enforce strong, complex passwords with a minimum of 8 characters including special characters
2. **Short Term:** Block the USB port on the Suprema biometric device using a physical port blocker to prevent data exfiltration
3. **Medium Term:** Implement adequate network segregation by creating a dedicated VLAN for biometric devices and ensure that it is not visible from other VLANs such as Production, Operations, Camera, Access Control, Routing, Radio and Default VLANs to restrict only authorized user access to the management console via internal network using access lists.
4. **Long Term (Optimum):** Implement a wireless intrusion prevention system that provides context-aware detection and correlation of unusual network activity and analyzes existing and zero-day threats in real-time against historical data.
5. **Long Term (Most Secure):** Implement an advanced forensics module that captures wireless activity and allows administrators the ability to rewind and analyze detailed records to support forensic investigation

Figure 2: Shows that USB port is available for data exfiltration

Figure 3: Shows that an attacker can delete trace of his

Figure 4: Shows the attacker can escalate privilege and access

Figure 5: Shows the potentially gaining access to fingerprint

Screenshot

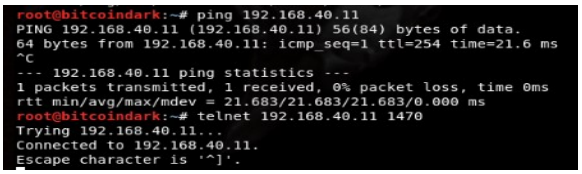


Figure 1

Figure 2

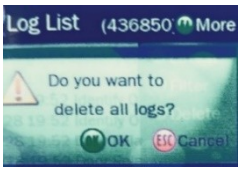


Figure 3

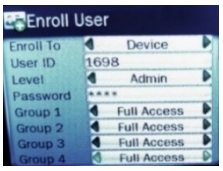


Figure 4

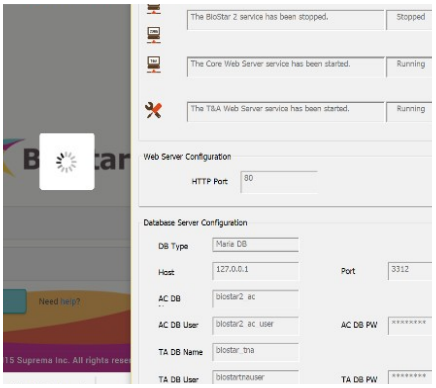


Figure 5

References

https://www.kensington.com/us/sg/4531/k67719us/usb-port-lock-with-rectangular-cable-guard

http://searchsecurity.techtarget.com/feature/Defeating-Evil-Twin-attacks?track=wsl3

1.4 Vulnerabilities exist in Wireless Controller

Score:

Description

During our assessment, we identified multiple vulnerabilities for in STC-Guest's WLAN controller including:
- A denial of service vulnerability within the AireOS software due to the presence of unsupported URLs in the web-based management interface and the improper handling of crafted Bonjour traffic
- A buffer overflow condition exists in the redirection functionality due to a failure to properly validate user-supplied input when handling HTTP requests.

Environmental Score	
Attack vector	Adjacent
Attack complexity	High
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	High
Remediation level	Official Fix
Report confidence	Confirmed

Affected Targets
Cisco Wireless

Impact

An unauthenticated, remote attacker can use a crafted request to one of the unsupported admin login URLs to cause the device to reload or execute arbitrary code. Arbitrary code execution is used to describe an attacker's ability to execute any command of the attacker's choice on a target machine or in a target process. From there the attacker can potentially take complete control over the machine the vulnerable process is running on. Hence an attacker may proceed to inject malicious code in order to gain access to sensitive information or disrupt the service.

Recommendation

1. **Interim Action:** Protect the WLAN controller from exploitation by implementing a CPU access control list (ACL) which can filter traffic destined for the management interface of the device
2. **Short Term:** Upgrade AireOS Software to Cisco's free update Release 7.6

   Upgrade WLC Software to Cisco's free update Release 8.0

Screenshot

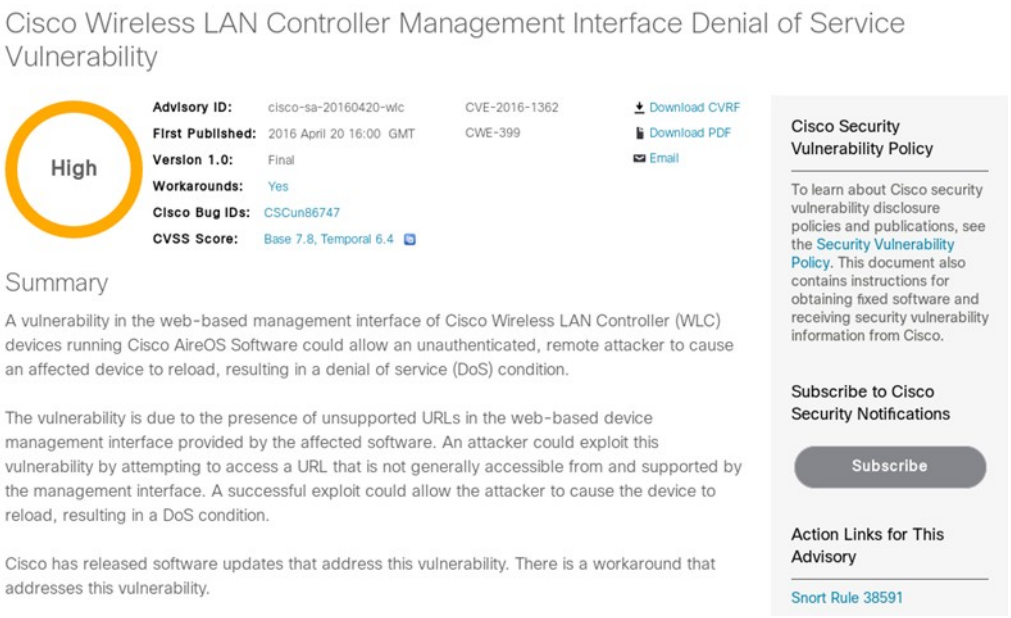


Figure 1: Nessus scan shows vulnerable services on WLAN Controller

Figure 1

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-wlc

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160420-bdos

1.5 Lack of Wi-Fi Jamming Protection

Score:

Description

Deauthentication attacks are used to disconnect all active users from a channel of an access point. By knowing the victim's MAC address, PwC could de-authenticate multiple clients from networks by sending de-authentication frames.

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High
Temporal Score	
Exploit maturity	High
Remediation level	Workaround
Report confidence	Confirmed

Impact

Failure in preventing deauth attack will eventually cause disruption to the network and create an unavailability of services and internet access. An attacker could potentially jam an entire wireless band creating huge service issues in J****'s Wi-Fi environment

Recommendation

1. a) **Interim Action**: Conduct periodic wireless audits using dedicated hardware

   b) **Short Term**: Passively monitor traffic with wireless intrusion detection systems distributed in the wireless network range

2. **Medium Term**: Enforce a corporate mobile device policy that only cellphones with a Wi-Fi 802.11 ac chipset will be supported for free wireless corporate internet

3. **Long Term (Optimum):** Enable Management Frame Protection (MFP) using the 802.11w protocol on Aruba OS 6.4 so that only authorized encapsulated deauthentication frames are valid and unencrypted deauthentication frames received by access points and clients from spoofed machines are invalid, dropped, and event logged by the wireless controller.

Affected Targets
All wireless devices

Screenshot

```
root@bitcoindark:~# aireplay-ng -a F0:5C:19:08:19:40 --deauth 0 wlan1mon
10:14:56  Waiting for beacon frame (BSSID: F0:5C:19:08:19:40) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
10:14:56  Sending DeAuth to broadcast -- BSSID: [F0:5C:19:08:19:40]
```

Figure 1

Figure 1: Show how wireless clients can be individually

References

http://www.willhackforsushi.com/papers/wlan-sess-cont.pdf

https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/5-2/wIPS/configuration/guide/msecg_wIPS/msecg_appA_wIPS.html

1.6 Wi-Fi signal leaks beyond official premise

Score:

Description

S******* Wi-Fi network is accessible from premises outside of J****'s physical control. Threat actors can detect S******* from common areas like the toilets, the lifts, and even from floors below including (29th floor smoking area & 33rd floor).

Impact

An attacker may be able to gain access from the-Wi-Fi signal that leaks out through J****'s fingerprint-protected doors, using a wireless adapter with a high-powered antenna. The attacker might gain access to S******* network through brute force or other methods and attempt to access sensitive information on servers and applications as the network is not segregated based on criticality. The attacker may also gain physical access via biometric device as it is accessible through the S******* network.

Environmental Score	
Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Affected Targets
S*******
STC_Guesst
STC_Corporate

Recommendation

1. **Short Term:** The signal strength of J****'s access points should be properly tuned with a conservative TX power that is sufficient to cover the appropriate space required.
2. **Long Term (Most Secure):** Paint exterior walls of J****'s office premises with wireless signal blocking paint made of tiny aluminum-iron oxide particles that prevent wireless Internet signals from being emitted outside the legal premises

Screenshot

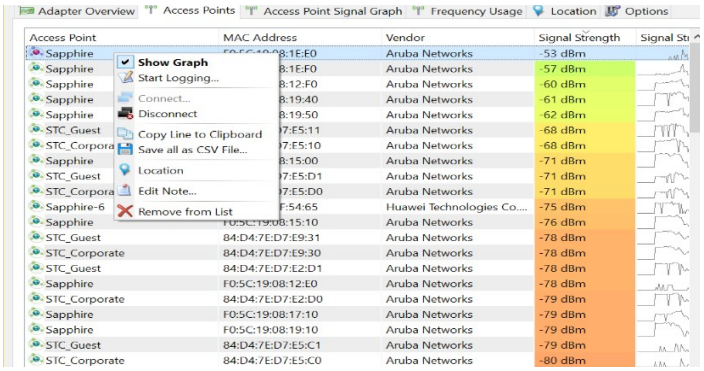
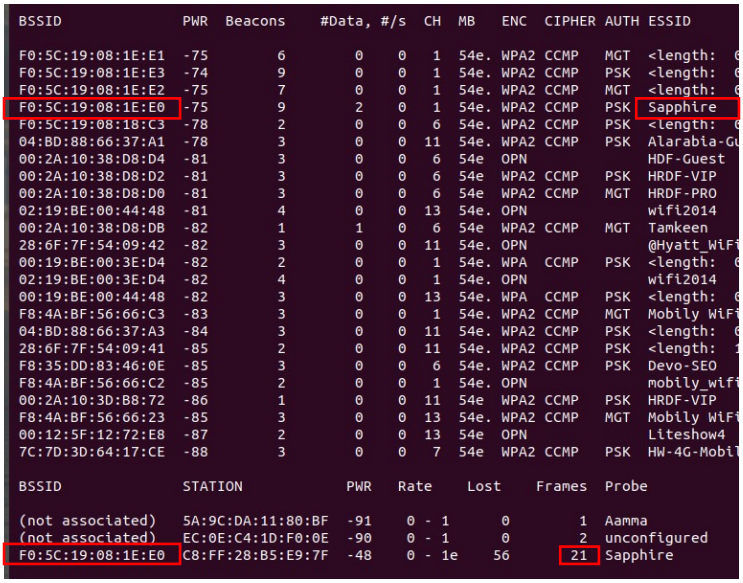


Figure 1

Figure 1: Signal strength scanner shows the available networks visible in the air from outside

Figure 2: Extremely strong signal of 75 decibel-



```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F0:5C:19:08:1E:E1  -75        6        0    0   1  54e. WPA2 CCMP   MGT  <length:  0
F0:5C:19:08:1E:E3  -74        9        0    0   1  54e. WPA2 CCMP   PSK  <length:  0
F0:5C:19:08:1E:E2  -75        7        0    0   1  54e. WPA2 CCMP   MGT  <length:  0
F0:5C:19:08:1E:E0  -75        9        2    0   1  54e. WPA2 CCMP   PSK  Sapphire
F0:5C:19:08:18:C3  -78        2        0    0   6  54e. WPA2 CCMP   PSK  <length:  0
04:BD:88:66:37:A1  -78        3        0    0  11  54e. WPA2 CCMP   PSK  Alarabia-Gu
00:2A:10:38:D8:D4  -81        3        0    0   6  54e  OPN              HDF-Guest
00:2A:10:38:D8:D2  -81        3        0    0   6  54e  WPA2 CCMP   PSK  HRDF-VIP
00:2A:10:38:D8:D0  -81        3        0    0   6  54e  WPA2 CCMP   MGT  HRDF-PRO
02:19:BE:00:44:48  -81        4        0    0  13  54e. OPN              wifi2014
00:2A:10:38:D8:DB  -82        1        1    0   6  54e  WPA2 CCMP   MGT  Tamkeen
28:6F:7F:54:09:42  -82        3        0    0  11  54e. OPN              @Hyatt_WiFi
00:19:BE:00:3E:D4  -82        2        0    0   1  54e. WPA  CCMP   PSK  <length:  0
02:19:BE:00:3E:D4  -82        4        0    0   1  54e. OPN              wifi2014
00:19:BE:00:44:48  -82        3        0    0  13  54e. WPA  CCMP   PSK  <length:  0
F8:4A:BF:56:66:C3  -83        3        0    0   1  54e. WPA2 CCMP   MGT  Mobily WiFi
04:BD:88:66:37:A3  -84        3        0    0  11  54e. WPA2 CCMP   PSK  <length:  0
28:6F:7F:54:09:41  -85        2        0    0  11  54e. WPA2 CCMP   PSK  <length:  1
F8:35:DD:83:46:0E  -85        3        0    0   6  54e. WPA2 CCMP   PSK  Devo-SEO
F8:4A:BF:56:66:C2  -85        2        0    0   1  54e. OPN              mobily_wifi
00:2A:10:3D:B8:72  -86        1        0    0  11  54e  WPA2 CCMP   PSK  HRDF-VIP
F8:4A:BF:56:66:23  -85        3        0    0  13  54e. WPA2 CCMP   MGT  Mobily WiFi
00:12:5F:12:72:E8  -87        2        0    0  13  54e  OPN              Liteshow4
7C:7D:3D:64:17:CE  -88        3        0    0   7  54e  WPA2 CCMP   PSK  HW-4G-Mobil

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   5A:9C:DA:11:80:BF  -91    0 - 1      0         1  Aamma
(not associated)   EC:0E:C4:1D:F0:0E  -90    0 - 1      0         2  unconfigured
F0:5C:19:08:1E:E0  C8:FF:28:B5:E9:7F  -48    0 - 1e    56        21  Sapphire
```

Figure 2

Figure 2: Successful frames indicate client is successfully accessing J****'s network from well outside the official

References

Critical High Medium **Low** Info

http://www.zdnet.com/article/the-real-value-in-anti-wifi-paint/

1.7 Lack of Protection against ICMP Tunneling

Score:

Description

ICMP tunnel allows us to set up one machine to receive TCP dumps and use another machine to successfully exfiltrate the contents of a 'confidential' PDF using ICMP. This is done by manipulating the maximum transfer unit of the link. Once exfiltrated, the data portion can be extracted from the ICMP dumps in hexadecimal format. This format can even be decoded into readable ASCII by programming in Python.

Impact

An attacker can create an ICMP tunnel as a covert connection between two endpoints by using ICMP echo requests and reply packets. This technique can allow an attacker to bypass the registration process using the one-time password on J****'s Guest Wi-Fi and simply tunnel their internet traffic through ICMP packets. Attackers most often plant a malicious device on an employee's device at the targeted premise to control and exfiltrate data through the tunnel to another machine, while still maintaining a low profile on the network traffic.

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None
Temporal Score	
Exploit maturity	Proof-of-concept
Remediation level	Workaround
Report confidence	Confirmed

Affected Targets
STC_Guest
S*******

Recommendation

1. a) **Short Term:** Block ICMP traffic from the J**** Guest Wi-Fi network.

   b) **Medium Term:** Allow fixed sized ICMP packets through firewalls.

Screenshot

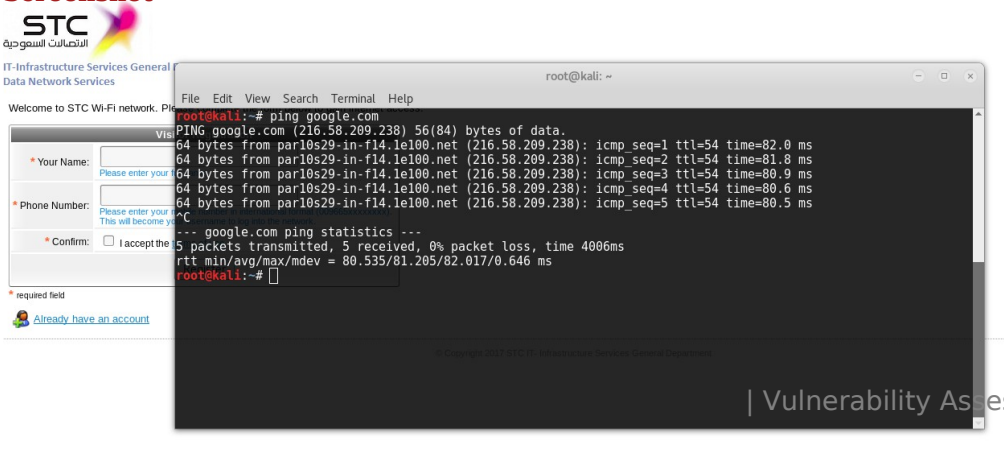


Figure 1: Shows ICMP packets can be sent out while on the Guest Wi-Fi

Figure 1

References
http://resources.infosecinstitute.com/icmp-attacks/

Critica High Medium **Low** Info

1.8 Lack of Protection against DNS Tunneling

Score:

Description

J****'s current Wi-Fi configuration allows intruders to perform DNS lookups by connecting their device to J****'s wireless network. It allows the attacker to encode data in the form of DNS queries and responses. DNS tunneling requires the compromised system to have external network connectivity, as DNS tunneling requires access to an internal DNS server with network access. Hackers must also control a domain and set up a name server that can act as an authoritative server to execute the server-side tunneling and data payload execution.

Impact

A DNS tunnel can be used for command and control data exfiltration or tunneling of any internet protocol (IP) traffic. Attackers use this technique to bypass the Wi-Fi authentication mechanism by tunneling their internet traffic through the DNS. This is potentially done by the adversary planting a malicious device on an employee's device and using it to control, and pull out compromised data through the tunnel, while maintaining a low profile. The attacker can potentially use the DNS tunnel to transmit data payloads to a target DNS server to command and control.

Environmental Score	
Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None
Temporal Score	
Exploit maturity	Proof-of-concept
Remediation level	Workaround
Report confidence	Confirmed

Affected Targets
STC_Guest
S*******

Recommendation

1. **Short Term:** Have internal hosts use a Web Proxy to handles resolution of all external domains.
2. **Medium Term:** Disable recursive DNS queries to external domains and

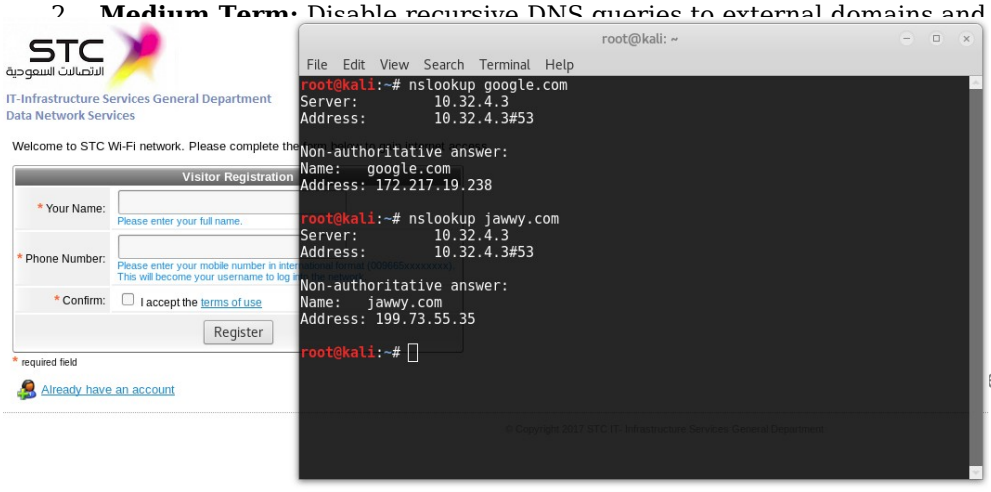


Figure 1: Shows DNS lookups can be conducted while on the Guest Wi-Fi.

Figure 1

References

https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152

Critical | High | Medium | **Low** | Info

1.9 Internal Webpages exposed inappropriately

Score:

Environmental Score	
Attack vector	Adjacent
Attack complexity	High
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	Low
Temporal Score	
Exploit maturity	Unproven
Remediation level	Workaround
Report confidence	Reasonable

Description

To login to the STC-guest network, user is required to input username and mobile to receive OTP to connect to the internet. However, while intercepting the traffic post login we found links to internal webpages where further internal login pages could be viewed. The Guest network is intended to be accessible for any guest, but due to the lack of segregation, attackers can connect to J****'s guest network and inappropriately penetrate the internal network.

Impact

An attacker can manually enter the IPs of web servers into the address field and gain access to the home screen of internal webpages. Once there, the attacker can attempt to crack admin or operator credentials and gain access to sensitive areas of Aruba's Access Management System. Once there, the attacker can tamper with network policies, configured devices, distributed security certificates, admit guest users, and even share information with third party solutions.

Recommendation

1. **Short Term:** Ensure that the guest network is segregated on a separate subnet from all other internal networks which contain J**** corporate systems.

2. a) **Medium Term:** Configure the firewall to drop packets directed at the internal network and only allow packets directed to the internet.

Affected Targets
cppmrdc.47wifi.s**.com.

b) **Long Term (Optimum):** Configure a unified threat management system to ensure connections from Guest WLAN IPs that are destined for internal IPs, to skip the proxy, so that the proxy server is only used to connect to external webs IPs.

Screenshot

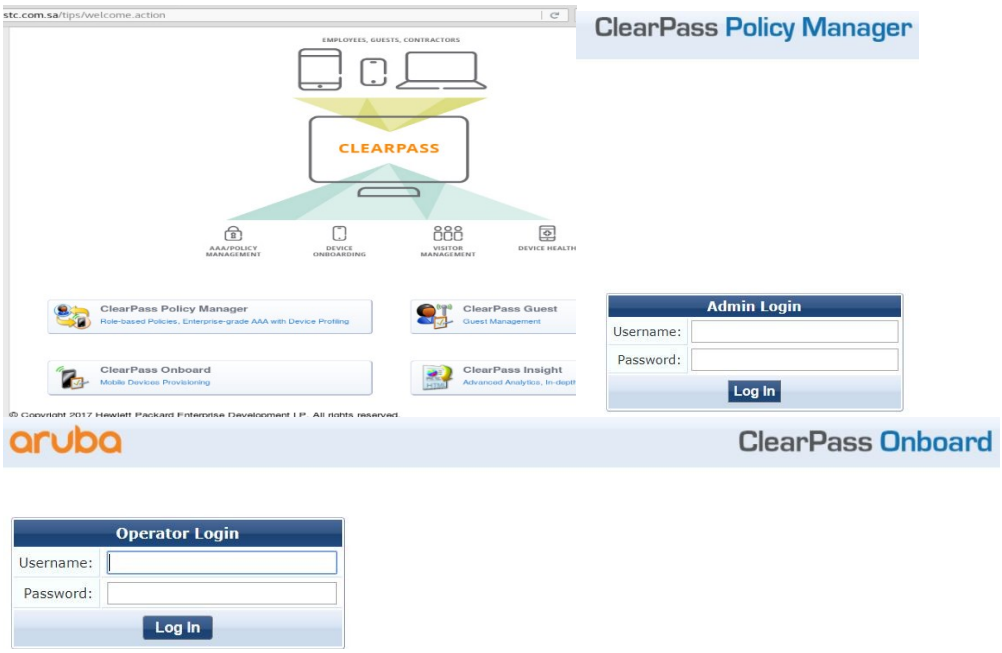


Figure 1: ClearPass Access Management Interface is available within intercepted traffic and allows browsing to various administrator and

Figure 1

References

https://community.sophos.com/products/unified-threat-management/f/web-protection-web-filtering-application-visibility-control/47012/block-access-from-a-guest-network-to-internal-networks

Critica High Medium **Low** Info

1.10 Rogue Access Points not monitored

Score:

Description

J**** is susceptible to the creation of multiple rogue access points which resemble authentic SSIDs and trick user devices to connect to them by emitting a stronger signal strength.

Environmental Score	
Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None
Temporal Score	
Exploit maturity	High
Remediation level	Workaround
Report confidence	Confirmed

Impact

A potential attacker or malicious insider can set up rogue access points to channel user traffic through their machine by launching variants of man-in-the-middle attacks, such as the 'Evil Twin'*. These variants include:

1. SSL strip to access passwords and credentials when victim authenticates to HTTPS websites such as Facebook and Gmail
2. SSH session compromise by posing as the target server and relaying client requests to the legitimate server.

3. DNS Spoofing to redirect a victim's web request to a legitimate registration page to a lookalike page on the attacker's local host, to solicit their credit card number.
4. Malicious responses served to the victim in the form of web pages containing embedded viruses or Trojans.

Affected Targets
J**** Premise

Recommendation

1. **Interim Action:** Increase employee awareness around the creation of rogue hotspots and options for using 802.1X in home WLANs.

   Conduct regular audits to detect duplicate SSID signals using access point discovery and site survey heat mapping tools to compare MAC addresses of participating wireless devices.

2. a) **Short Term:** Implement a wireless vulnerability assessment module that allows administrators the ability to automatically log on to access points and test for vulnerabilities.

   b) **Medium Term:** Implement a wireless security compliance suite that monitors specified radio spectra to detect and neutralize rogue devices, enforce wireless policies and ensure regulatory compliance.

3. **Long Term (Optimum):** Implement a wireless intrusion prevention system that provides context-aware detection and correlation of unusual network activity and analyzes existing and zero-day threats in real-time against historical data. Have administrators track Rogue APs id via IPS' integrated over-the-air physical location capabilities.

4. **Long Term (Most Secure):** Supplement IPS with alarms such as Karma tool detection and implement an advanced forensics module that captures wireless activity and allows administrators the ability to rewind and analyze detailed records to support forensic investigation

Figure 1: Shows SSL strip attack that sniffs usernames and passwords from a secure https login

Screenshot

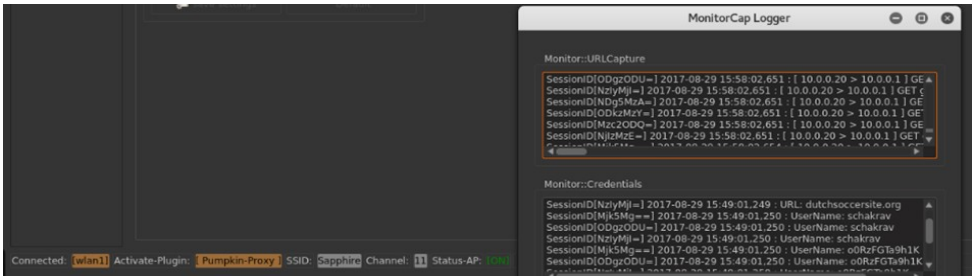


Figure 1

References

http://www.cisco.com/c/en/us/support/docs/wireless-mob ss-lan-wlan/7028

Critica High Medium **Low** Info

https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-4/wIPS_Configuration/Guide/7_4_MSE_wIPS/7_4_MSE_wIPS_appendix_01100.html

1.11 Users' Beacon messages are leaked

Score:

Description

J**** allows collection of beacon messages as part of an attacker's research into exploitation of users' device connectivity. Attackers will collect beacon messages as part of the reconnaissance phase to initiate attacks on user devices.

Impact

The reconnaissance allows the attacker to know the name of the access point that the user has already saved on their device and by extension one which will connect to automatically without further intervention. Additionally, the

Environmental Score	
Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	None
Temporal Score	
Exploit maturity	High
Remediation level	Workaround
Report confidence	Confirmed

attacker can cause a denial of service on an access point by forcing it into continuously responding to a constant stream of wireless packets and be unable to serve legitimate clients.

Recommendation

1. **Interim Action:** Raise awareness amongst employees and government officials to remove saved networks and turn off Wi-Fi in transit to prevent their phone exposing network names along the way.
2. **Medium:** Ensure intrusion prevention capabilities monitor levels of probe request frames and triggers a probe request flood alarm when the threshold is exceeded.
3. **Long Term (Optimum):** Deploy initiative to provide corporate devices to employees to connect to workplace Wi-Fi. Issue the latest mobile hardware that take precautions against probe request as part of their inherent design.
4. **Long Term (Most Secure):** Implement an enterprise mobile policy that geofences when Wi-Fi can be turned on corporate devices, so internal access point names are not exposed to allow man-in-the-middle attacks on sensitive applications.

Affected Targets

Endpoints and devices

Screenshot

```
root@kali:~/tools# ./hoover.pl --interface wlan1mon --tshark-path /usr/bin/tshark
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to runn
superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help
ark as an unprivileged user.
Capturing on 'wlan1mon'
4 ++ New probe request from ac:18:26:2d:80:6f with SSID: SAPPHIRE_VIP [1]
25 ++ New probe request from 80:00:0b:96:b2:b6 with SSID: Sapphire [2]
95 ++ New probe request from e4:a7:a0:75:40:31 with SSID: Alfahad [3]
++ New probe request from e4:a7:a0:75:40:31 with SSID: JW-CC-TECH [4]
116 ++ New probe request from 06:08:a1:82:cd:b1 with SSID: Wireless [5]
++ New probe request from 64:5a:04:ac:ad:0e with SSID: Alarabia-Staff [6]
146 ++ New probe request from ac:5f:3e:dd:ba:47 with SSID: OMAR [7]
160 ++ New probe request from b0:72:bf:7a:c7:73 with SSID: malek [8]
195 ++ New probe request from c2:a8:07:70:f8:05 with SSID: mobilywifi [9]
255 ++ New probe request from c0:ee:fb:d7:b4:bc with SSID: HUAWEI-E5372-0B56 [10]
++ New probe request from c0:ee:fb:d7:b4:bc with SSID: YDXJ_3855028 [11]
297 ++ New probe request from 20:55:31:cc:40:09 with SSID: JW-CCIT [12]
484 ++ New probe request from 44:80:eb:7f:45:64 with SSID: JAWWY-TR [13]
549 ++ New probe request from a8:66:7f:19:89:b1 with SSID: b.a.m [14]
810 ++ New probe request from 60:a4:d0:59:78:c4 with SSID: .. [15]
```

Figure 1

Figure 1: Shows probe requests from various user devices to surrounding Wi-Fi networks being exposed and tracked

References

https://arstechnica.com/information-technology/2014/11/where-have-you-been-your-smartphones-wi-fi-is-telling-everyone/

https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-2/wIPS_Configuration/Guide/wIPS_72/msecg_appA_wIPS.html

1.12 Lack of Client to Client Segregation

Score:

Description

J****'s current Wi-Fi setup allows a connected client to ping other clients in J****'s wireless network and to run some scans on other clients.

Environmental Score	
Attack vector	Network
Attack complexity	High
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None
Temporal Score	
Exploit maturity	High
Remediation level	Official Fix
Report confidence	Confirmed

Impact

An attacker may attempt to compromise other clients who are connected to the same wireless
network and extend its attack vector.

Recommendation

1. a) **Medium Term:** Configure the wireless controller to segregate the users. This can be done by denying inter-user bridging. If possible segregate the categories of users (e.g. system administrators, employees, third parties, VIP, etc.) in different VLANs.

   b) **Medium Term:** Enable public secure packet forwarding (PSPF) to prevent client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point.

Affected Targets

S*******
II-CC-Tech

Screenshot

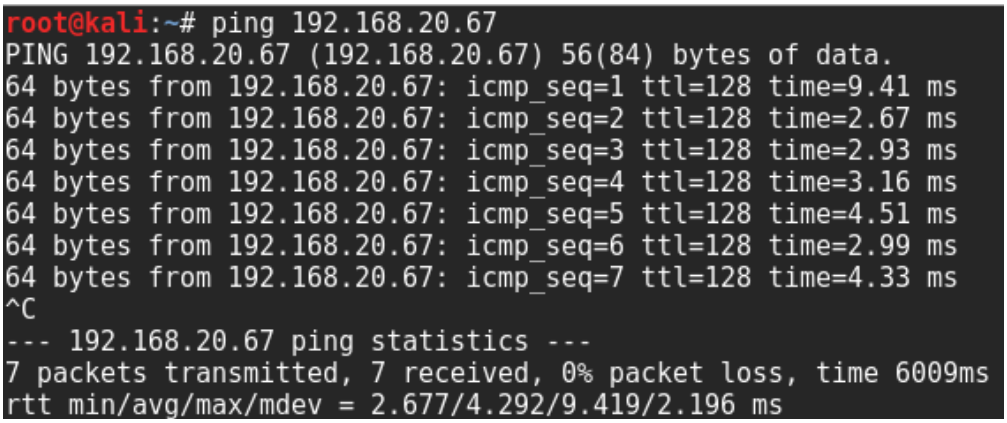


Figure 1

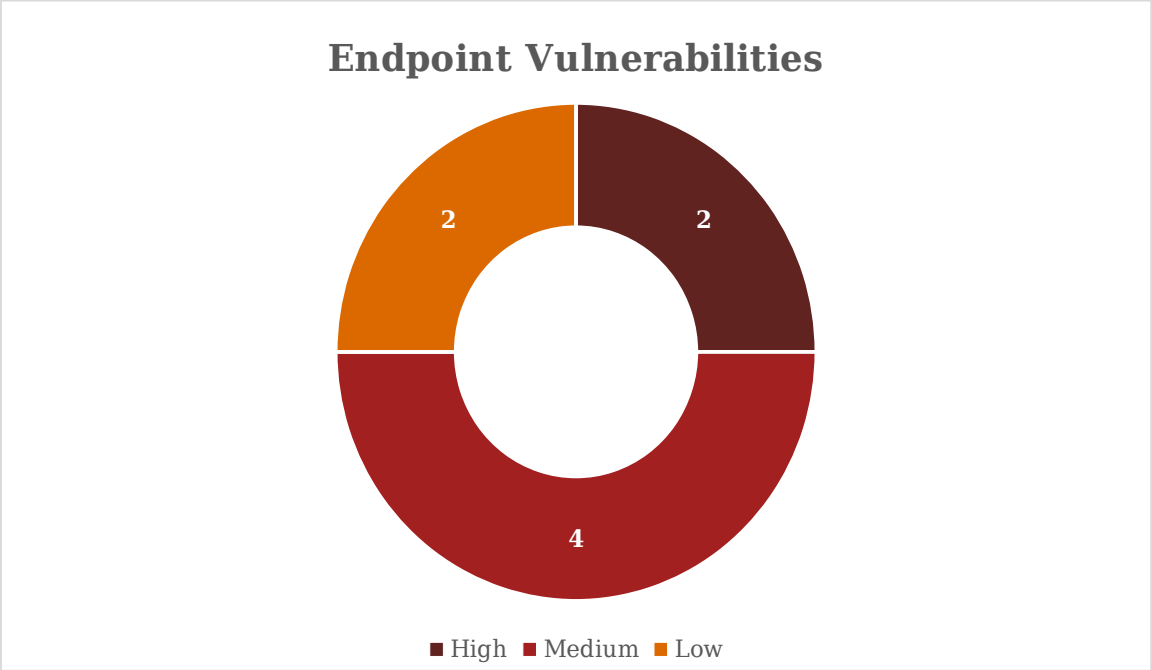
Figure 1: Shows the IP address of a client connected to the same WLAN segment can be queried for a successful connection

References

http://community.arubanetworks.com/t5/Controllerless-Networks/Wi-Fi-client-segregation-per-SSID/td-p/204887

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4_21a_JA1/configuration/guide/scg12421aJA1/scg12421aJA1-chap6-radio.html#wp1038494

2. Endpoint Security Assessment



Laptops Serial Number Tested

1. **Lenovo** – PF-0E29LT 15/11
2. **MAC** – C1MR71P4DTY3

2.1 Absence of Malware Protection

Score:

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Description

The standard J**** endpoint does not have a specialized anti-malware solution beyond the packaged Windows Defender that is natively installed to protect it from the latest virus definitions and advanced persistent threats. A comprehensive anti-virus suite provides the endpoint with web URL filtering, real-time malware protection that includes an anti-ransomware layer, vulnerability scanning and exploit protection, modules to protect against phishing and PowerShell attacks, aids with automated password creation and management, shreds files that contain classified information, and controls external device access to USBs, external hard drives, optical storage media, even those that connect by Bluetooth.

Impact

Without a centralized anti-malware engine, controlled by a threat-monitoring agent, J****'s endpoints have no consistent security posture and are left open to bugs, worms, trojan horses, adware and spyware present on the Internet. These debilitating bugs and viruses will cause users' computers to malfunction and leak personally identifiable information. Moreover, the user remains exposed to dangerous sites, search engine results, malicious scripts, risk of financial transactions being exposed, and other malevolent intrusions.

Recommendation

1. **Interim Action:** Implement antispyware software that runs constantly in the background to block spyware installation regardless of source, on the endpoint.
2. **Short Term:** Implement an antimalware product that combines signature-based scanning with heuristics technology and cloud-based global threat intelligence to recognize and root out malware on J**** endpoints.
3. **Medium Term:** Implement website browsing protection using the latest reputation technology that consults with rating databases and blocks the user browsing to websites reported as unsafe
4. **Long Term (Optimum):** Implement device control to enable IT to restrict or block user access by setting and enforcing device access rules in accordance with J****'s work culture and policy

References

http://www.techradar.com/news/top-5-best-business-anti-malware-and-anti-spyware-software

http://searchsecurity.techtarget.com/feature/Fundamentals-of-endpoint-security-Antimalware-protection-in-the-enterprise

2.2 Lack of Full-Disk Encryption

Score: 

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Description

As J**** has a digitally open culture it is possible that employees might store information on their machines including customer sensitive information and personal information. However, we have noticed that the machines are not protected using full disk-based encryption.

Impact

Without disk-based encryption, a laptop that is stolen can have its hard drive harvested and connected to a different machine to bypass existing authentication mechanisms. This can lead to the breach of critical client data and result in the potential loss of customer confidence, litigation concerns, and bad press. Hard-drive encryption allows files to be automatically encrypted when written to the drive and decrypted when being read from the drive. The encryption and decryption processes are transparent to applications such as word processors, databases, spreadsheets and imaging programs.

Recommendation

Interim Action: Implement software-based full disk encryption (FDE) to encrypt bootable disk partitions using trusted algorithms such as Advanced Encryption Standard (AES) with 256-bit key lengths.

Short Term: Supplement FDE with file/folder encryption.

Medium Term: Security team collaborates with IT administrators to defines policies on a central management server which are pushed down to user system encryption agents.

Long Term (Optimum): Enhance FDE with hardware-based trusted platform module (TPM) chips to encrypt master boot records (MBR) for additional security without affecting system stability and performance.

Long Term (Most Secure): Granularize policies to be based on file types and more content-driven to integrate with prospective data loss prevention solution.

References

http://searchsecurity.techtarget.com/magazineContent/Use-full-disk-or-file-folder-encryption-for-laptop-data-security

http://searchenterprisedesktop.techtarget.com/definition/hard-drive-encryption

2.3 Detection of SMB Vulnerabilities

Score:

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Description

The standard J**** endpoint is affected by multiple SMB related vulnerabilities. These include the Windows SMB remote code execution vulnerability on Microsoft server message block 1.0 (SMBv1) and the Windows SMB denial of service vulnerability.

Impact

An attacker may exploit SMB related vulnerabilities to create a denial of service or compromise the system. These vulnerabilities can also be used to upload malicious files to infect the system. Eventually the attacker might be able to gain access to the endpoint machine or at least disrupt the employee's work.

Recommendation

Interim Action: Install official SMB updates as per vendor advisory

Short Term: Setup system centre configuration manager in a two-server farm for patch management of all J**** corporate devices.

Medium Term: Integrate SCCM with specialized third-party patch-management solution with value-added services such as on-demand patching, filtered views, and application-specific configuration patching for third-party suites such as Java, Adobe etc.

Long Term (Optimum): Enable Wake-on-WAN feature and global scheduling to ensure that devices are patched immediately over client VPN regardless of geographic location.

Long Term (Most Secure): Supplement patching solution with premium features such as advanced analysis reports of installed endpoint applications, antivirus optimization and firewall port tuning and file share permission configuration.

References

http://www.securityfocus.com/bid/98272/info

http://www.securityfocus.com/bid/98274/info

http://searchsecurity.techtarget.com/feature/Discover-the-best-patch-management-software-for-your-business

http://www.networkmanagementsoftware.com/five-great-patch-management-tools/

Critica High **Medium** Low Info

2.4 Local Administrator is not protected

Score:

Environmental Score	
Attack vector	Physical
Attack complexity	Low
Privileges required	High
User interaction	Required
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Description

The standard J**** endpoint allows the default user administrative privileges on the endpoint, allowing them full access to modify the system. An employee can also perform tasks not required for their role including installing software, transferring files through USB, disabling antivirus and/or updates, etc.

Impact

With administrative privileges, malicious files can overwrite or modify critical system configurations, deactivate security features and make the system vulnerable to different attacks.

Recommendation

Interim Action: for critical users, schedule corporate device audit, manually remove local administrator accounts privileges, and replace with an account with fewer privileges (e.g. Windows “Standard User”.

Short Term: Complete Active Directory setup and set up group policies to generate privilege elevation and application control for users based on security groups.

Medium Term: Enable automated analysis of unknown applications and greylisting them to safely run in restricted mode.

Long Term (Optimum): Implement threat detection capabilities to block malicious executables from propagating and running on all computers.

Long Term (Most Secure): Implement behavioral analysis to detect attempted theft of windows credentials.

Screenshot

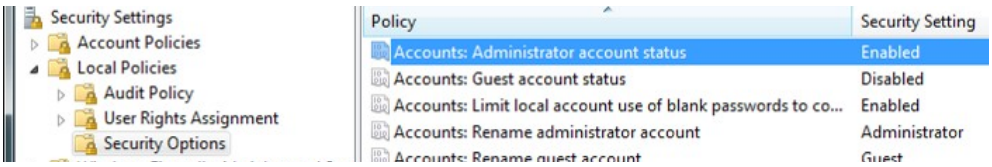


Figure 1

Figure 1: Shows the user can access local group policy and elevate himself to

References

https://www.networkworld.com/article/2190847/network-security/best-practices-for-endpoint-security--part-1.html

https://www.cyberark.com/products/privileged-account-security-solution/endpoint-privilege-manager/

https://helpdeskgeek.com/windows-7/turn-off-admin-approval-mode-in-windows-7/

Critica High **Medium** Low Info

2.5 Unsecured BIOS Setup

Score:

Environmental Score	
Attack vector	Physical
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Description

Secure Boot is a component to help prevent malicious software applications and unauthorized operating systems from loading during the system start-up process. It ensures that the machine boots using only firmware that is trusted by the manufacturer. However, we have noticed that the standard J**** machine has secure Boot Mode disabled.

Impact

Without Secure Boot enabled, an attacker without valid Windows credentials can use physical access to hijack the endpoint by employing malicious software via unauthorized media to load into an operating system and bypass the default boot process.

Recommendation

Interim Action: Enable Unified Extensible Firmware Interface (UEFI) on J**** endpoint before issuing them to employees. UEFI supports networking features natively in the firmware to allow administrators the ability to remotely troubleshoot and harden configuration.

Short Term: Centrally manage all J**** endpoint BIOS settings from a secure image that enables Secure Boot as default to ensure that all J**** machines boot using firmware that is trusted by the manufacturer. Secure boot allows the operating system to be checked for tampering during boot process.

Screenshot

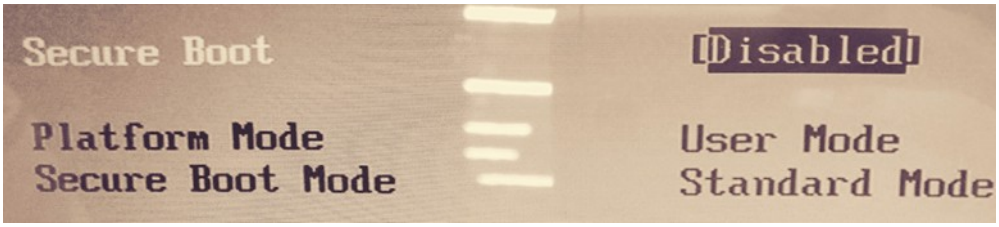


Figure 1

Figure 1: Shows the endpoint does not have secure boot

References

http://www.makeuseof.com/tag/what-is-uefi-and-how-does-it-keep-you-more-secure/

https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/boot-to-uefi-mode-or-legacy-bios-mode

Critical | High | **Medium** | Low | Info

2.6 Absence of Data Leakage Protection

Score: 

Description

The standard J**** endpoint does not currently have DLP solution in place to control the transfer of sensitive data. This means that users can import and export any file or folder out of the endpoint without being tracked, through one of a multitude of options at their disposal: USB, Ethernet, Bluetooth, Mobile Networks, Wi-Fi, FTP, screenshots etc.

Environmental Score	
Attack vector	Physical
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	Low
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Impact

As J**** allows multiple consultants and third-party vendors to utilize company resources such as their Wi-Fi network, laptops with privileged access, it is possible for sensitive company data to be exfiltrated without detection by a malicious insider, due to inadequate control implementation.

Recommendation

Interim Action: Implement a DLP solution in the network with content-aware detection capabilities that identifies data in multiple formats by fingerprinting structured data sources and looking for matches between keywords, expressions, patterns and file properties. Based on the J**** context, it's suggested to configure the DLP in monitoring mode to support the incident management and security monitoring processes.

Short Term: Expand DLP solution into a full data classification suite which includes full mobile security functionality to prevent users downloading confidential material to their untrusted devices.

Medium Term: Implement protection of data in motion by detecting confidential information over HTTP, FTP, SMTP, custom port-specific protocols and providing thorough content inspection of all communications without packet loss.

Long Term (Optimum): Implement advanced features into DLP including exact match, regex with validation, custom keyword dictionaries, global data identifiers, Boolean operators, and Luhn checks.

Long Term (Most Secure): Supplement DLP with watermarking software that includes screen capture, keystroke logging, clipboard remote access, webcam and microphone hijacking protection.

References

https://securitywing.com/data-exfiltration-prevention-tips/

https://www.symantec.com/connect/blogs/7-must-haves-your-next-dlp-system

Critical | High | **Medium** | Low | Info

2.7 Vulnerabilities in Evoko Meeting Management Devic

Score:

Description

During our analysis, we found that the smart meeting room booking system, Evoko Liso could be accessed by an attacker. The attacker can gain administrative access and reboot into a customized Linux system from a USB drive by touching the screen during the reboot process. Through vulnerabilities in the endpoint Evoko Liso device an attacker, gain access to the connected Evoko Home server and jump into J****'s network due to the lack of network segregation.

Environmental Score	
Attack vector	Physical
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	Low
Integrity	Low
Availability	Low
Temporal Score	
Exploit maturity	Proof-of-concept
Remediation level	Temporary
Report confidence	Reasonable

Impact

The attacker can execute arbitrary shell commands with root privileges in the booted system.
There is no protection against reading or modifying the existing file system of the device, which means that an attacker can steal configuration data and install any executable code on the system. The attacker will only need temporary access (1-5 minutes) to install a permanent backdoor on the system that will remain even after a normal firmware update. The only way to erase such backdoors would be to run a full firmware factory reset over USB. Such attacks can happen before or after the device has been installed outside a conference room. An attacker with network access to the Evoko Home application can even use built-in functionality to send malicious email with content and recipients specified by the attacker.

Recommendation

Interim Action: Change the default administrator credentials on the system to prevent the attacker from rebooting operating system.

Affected Targets
Evoko Meeting Room Management Devices

Short Term: Block the USB port on the Evoko smart meeting room booking system device using a physical port blocker to prevent the attacker from booting into an offensive operating system.

Medium Term: Upgrade all systems to latest official Evoko firmware version 1.30 or above.

Screenshot

Figure 1: Shows the attacker can gain access to the facility admin screen from where the operating system can be

Figure 1

References

https://truesecdev.wordpress.com/2017/04/27/vulnerabilities-in-evoko-products/

http://www.securityweek.com/flaws-found-evoko-meeting-room-management-devices

Critica Hig Medium Low Info

2.8 MacBook user authentication bypass exists

Score:

Description

Affected Targets
Mac books

A thieving attacker or malicious insider can gain access to a J**** MacBook by bypassing the user account password by booting into Recovery Mode from startup

Environmental Score	
Attack vector	Physical
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	None
Temporal Score	
Exploit maturity	High
Remediation level	Official Fix
Report confidence	Confirmed

Impact

An attacker can gain access to sensitive corporate data or even wipe the system clean and begin using it as their own

Recommendation

1. a) **Interim Term:** Ensure all provisioned MacBooks have FileVault encryption enabled and employees are required to sign a form to securely store the recovery key need to reset the password. This thorized users from access files and folders even if they into the Apple operating system

b) **Short Term:** Ensure all provisioned MacBooks have enabled firmware passwords. This hardware-based encryption tool ensures that a password is required to boot into Recovery Mode or from an external drive. This prevents unauthorized users from listing user accounts on a machine and changing their passwords

Screenshot

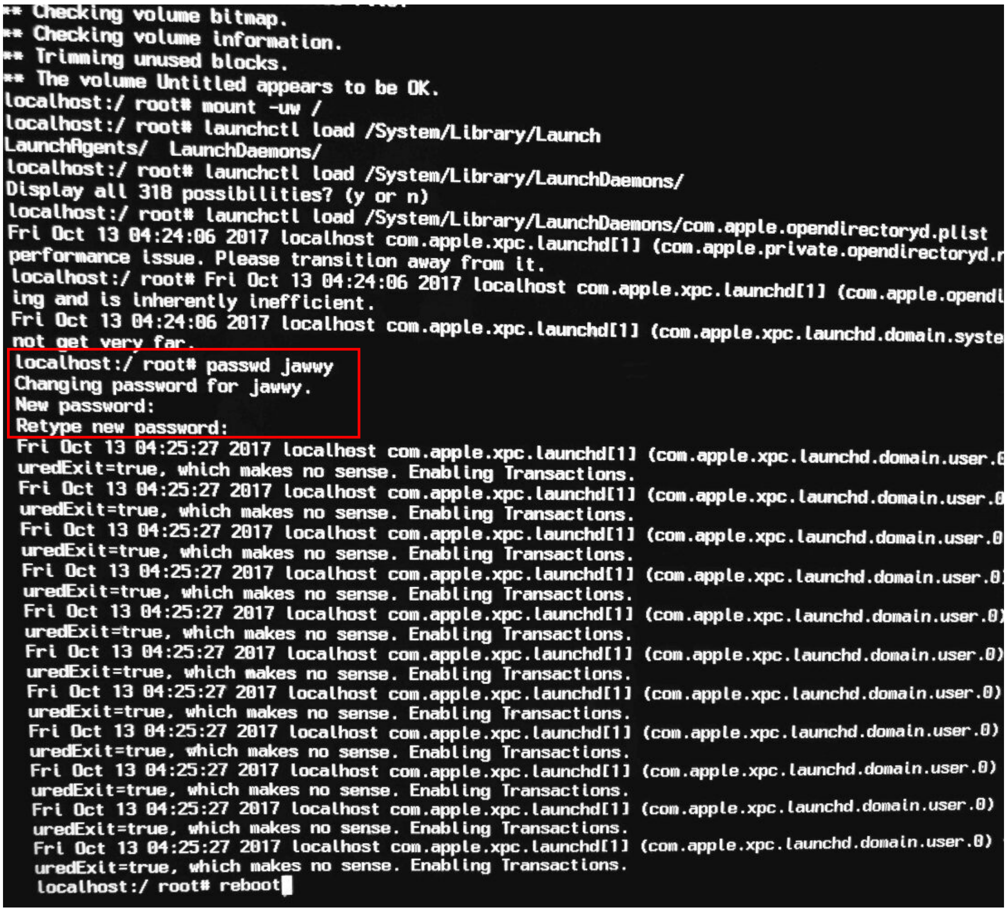


Figure 1

Figure 1: Shows how the user password can be easily bypassed from recovery without the need for external

References

https://www.cnet.com/how-to/prevent-your-mac-password-from-being-bypassed/

https://www.howtogeek.com/209672/anyone-with-access-to-your-mac-can-bypass-your-password-unless-you-do-this/amp/

3. Win7 Configuration Assessment

Objective

The following endpoint configuration scan helps to provide S******* with an overview of key misconfigurations in a typical Windows 7 machine used by an employee. The results may not accurately reflect the state of every single user machine. The misconfigurations are mapped to a CCE number which used to find the corresponding mapping at the official listing of:

https://cce.mitre.org/lists/cce_list.html

The Windows 7 .xls file on the link provides further details on each CCE, the parameters available, what the setting means, where its registry key is located etc.

CCE ID	CCE Description	CCE Parameters	CCE Technical Mechanisms	Management Toolkit for Windows 7, Version 1.0: "Windows 7 Security Baseline.xml"
CCE-10061-0	The 'Turn off printing over HTTP' setting should be configured correctly.	enabled/disabled	(1) GPO: Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP (2) Registry Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\DisableHTTPPrinting	Setting Index #240: This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet.

Background

The CCE List provides unique identifiers to security-related system configuration issues to improve workflow by facilitating fast and accurate correlation of configuration data across multiple information sources and tools.

CCE is one of six existing open standards used by NIST to help automate vulnerability management and evaluate compliance with federal information technology security requirements.

Why CCE

When dealing with information from multiple sources, use of consistent identifiers improve data correlation; enable interoperability; foster automation; and ease the gathering of metrics for use in situation awareness, IT security audits, and regulatory compliance.

CVE vs. CCE

Like CVE, CCE assigns a unique, common identifier to a security-related configuration issue. CCE identifiers are associated with configuration statements controls that express the way humans name and discuss their intentions when configuring computer systems. The use of CCE-IDs as tags provide a bridge between natural language, prose-based configuration guidance documents and machine-readable or executable capabilities such as configuration audit tools.

Community

CCE is industry-endorsed through the CCE Working Group which includes members from major operating systems vendors, commercial information security tool vendors, academia, government agencies, and research institutions.

3.1 Misconfigurations in Password Policy Settings

S#	Issue	CCE
1	"Enforce password history" should meet minimum requirements of passwords remembered	8912
2	The 'Minimum password age' should be configured to the correct number of days	9330
3	The 'Minimum password length' should be configured to the correct number of characters	9357
4	The 'Password must meet complexity requirements' should be set correctly	9370

3.2 Misconfigurations in User Rights Assignments

S#	Issue	CCE
5	'Access this computer from the network' should be assigned to the appropriate accounts	9253
6	'Allow log on locally' should be assigned to the appropriate accounts	9345
7	The 'Back up files and directories' should be assigned to the appropriate accounts	9389
8	The 'Bypass traverse checking' should be assigned to the appropriate list accounts	8414
9	The 'Deny log on as a batch job' should be assigned to the appropriate list of accounts	9212
10	The 'Deny log on through Remote Desktop Services' should be assigned to the appropriate accounts	9274
11	The 'Increase a process working set' should be assigned to the appropriate accounts.	9048
12	The 'Restore files and directories' should be assigned to the appropriates list of accounts	9124
13	The 'Shut down the system' should be assigned to the appropriate list of accounts	9014

3.3 Misconfigurations in Security Options

S#	Issue	CCE
14	Force audit policy subcategory to override audit policy category should be enabled	9432
15	Interactive logon: Do not display last user name setting should be enabled	9449
16	Do not require CTRL+ALT+DEL' setting should be disabled	9317
17	Interactive logon Message text for users attempting to log on should be configured correctly	8973
18	Number of previous logons to cache in the absence of domain controller should be configured correctly	8487
19	Prompt user to change password before expiration should be enabled	9307
20	Anonymous enumeration of SAM accounts should be disabled	9156
21	Disable storage of passwords and credentials for network authentication	8654
22	Disable shares that can be accessed anonymously	9196
23	Enable local system to use computer identity for NTLM	9096
24	Disallow Local System NULL session fallback	8804
25	Disallow PKU2U authentication requests to this computer to use online identities	9770
26	Force logoff when logon hours expire	9704
27	LAN Manager authentication level' should be disabled	8806
28	Enable the use of FIPS compliant algorithms for encryption, hashing, and signing	9266
29	Enable consent for elevation prompt in Admin Approval Mode	8958
30	Disable Automatic Logon	9342
31	Disable IP source routing to protect against packet spoofing	9496
32	Disallow ICMP redirects to override OSPF generated routes	8513
33	Hide Computer From the Browse List	8560
34	Set Keep Alive Time for packets to 300,000 milliseconds	9426
35	Enable No Default Exempt for IPSec Filtering	9439
36	Allow computer to ignore NetBIOS name release requests except from WINS servers	8562

37	Disable Internet Router Discovery Protocol (IRDP) used to configure default gateway addresses	9458
38	Enable Safe DLL search mode	9348
39	Configure the time in seconds to 0 before the screen saver grace period expires	8591
40	Reduce registry value entry for maximum unacknowledged data retransmission to 3	9456
41	Configure percentage threshold for the security event log to generate a warning" to 90	9501

3.4 Misconfigurations in System Services

S#	Issue	CCE
42	Disable Bluetooth Support Service	10661
43	Disable Home Group Listener Service	10543
44	Disable Parental Controls Service	10311

3.5 Misconfigurations in Audit Policies

S#	Issue	CCE
45	Auditing of events should be enabled	9498
46	Detailed Tracking of Process Creation events should be enabled	9562
47	Auditing of Account Lockout events should be enabled	8853
48	Auditing of Logon-Logoff events should be enabled	9683
49	Auditing of Object Access File System should be enabled	9217
50	Auditing of Audit Policy Change events should be enabled	10021
51	Auditing of Sensitive Privilege Use events should be enabled	9878
52	Auditing of IPsec Driver events should be enabled	9925
53	Auditing of Other System events should be enabled	9586
54	Auditing of Security State Change events should be enabled	9850
55	Auditing of Security System Extension events should be enabled	9863

3.6 Misconfigurations in Network Connections

S#	Issue	CCE
56	“Turn on Mapper I/O (LLTDIO) Driver” setting should be configured correctly	9783
57	“Turn on Responder (RSPNDR) Driver “setting should be configured correctly	10059
58	Startup of Microsoft Peer-to-Peer Networking Services should be configured correctly	10438
59	Installation and Configuration of Network Bridge on the DNS Domain Network should be configured correctly	9953
60	“Require domain users to elevate when setting a network's location’ setting should be configured correctly	10359
61	“Route all traffic through the internal network” setting should be configured correctly	10509
62	“6to4 State” setting should be configured correctly	10266
63	“ISATAP State” setting for IPv6 should be configured correctly	10130
64	“Teredo State” setting should be configured correctly	10011
65	“IP HTTPS” state setting should be configured correctly	10764
66	“Configuration of wireless settings using Windows Connect Now” setting should be configured correctly for Wireless Connect Now over Ethernet (UPnP)	9879
67	“Prohibit Access of the Windows Connect Now Wizards” setting should be configured correctly	10778
68	“Extend Point and Print connection to search Windows Update and use alternate connection if needed” setting should be configured correctly	10782

3.7 Misconfigurations in System Settings

S#	Issue	CCE
69	“Allow remote access to the PnP interface” setting should be configured correctly	10769
70	“Do not send a Windows Error Report when a generic driver is installed on a device” setting should be configured correctly	9901

71	“Do not create system restore point when new device driver installed” setting should be configured correctly	10553
72	“Prevent device metadata retrieval from internet” setting should be configured correctly	10165
73	“Specify Search Order for device driver source locations” setting should be configured correctly	9919
74	“Registry Policy Processing” setting should be enabled	9361
75	“Turn off downloading of print drivers over HTTP” setting should be configured correctly	9195
76	“Turn Off Event Views ‘Events.asp’ Links” setting should be configured correctly	9819
77	“Turn Off Handwriting Recognition Error Reporting” setting should be configured correctly	10645
78	“Turn Off Internet Connection Wizard if URL Connection is Referring to Microsoft.com” setting should be configured correctly	10649
79	“Turn off Internet download for Web publishing and online ordering wizards” setting should be configured correctly	9674
80	“Turn Off Internet File Association Service” setting should be configured correctly	10795
81	“Turn off printing over HTTP” setting should be configured correctly	10061
82	“Turn off Search Companion content file updates” setting should be configured correctly	10140
83	“Turn Off the ‘Order Prints’ Picture Task” setting should be configured correctly	9823
84	“Turn off the ‘Publish to Web’ task for files and folders” setting should be configured correctly	9643
85	“Turn off the Windows Messenger Customer Experience Improvement Program” setting should be configured correctly	9559
86	“Enable Error Reporting” policy should be set correctly	10441
87	Use Classic Logon should be properly configured	10591
88	“Do not process the run once list” setting should be configured correctly	10154
89	“Require a Password When a Computer Wakes” setting should be configured correctly	9829
90	Unsolicited offers of remote assistance should be automatically rejected or passed to the logged-on user for confirmation as appropriate	9960
91	“Turn on session logging” setting should be configured correctly	1034

		4
92	“Restrictions for Unauthenticated RPC clients” setting should be configured correctly	9396
93	“RPC Endpoint Mapper Client Authentication” setting should be configured correctly	10181

3.8 Misconfigurations in Troubleshoot & Diagnostics

S#	Issue	CCE
94	“Turn on Microsoft Support Diagnostic Tool interactive communication with support provider” setting should be configured correctly	9842
95	“Troubleshooting: Allow user to access online troubleshooting content on Microsoft servers from the Troubleshooting Control Panel” setting should be configured correctly	10606
96	“Enable/Disable PerfTrack” setting should be configured correctly	10219

3.9 Misconfigurations in Windows Components

S#	Issue	CCE
97	“Configure Windows NTP Client\NTP Server” setting should be configured correctly	10500
98	“Turn off Program Inventory” setting should be configured correctly	10787
99	The default behavior for AutoRun should be properly configured	10527
100	“Enumerate administrator accounts on elevation” setting should be configured correctly	9938
101	“Do not allow Digital Locker to run” setting should be configured correctly	10759
102	“Override the More Gadgets Link” setting should be configured correctly	9857
103	“Disable unpacking and installation of gadgets that are not digitally signed” setting should be configured correctly	10811
104	“Turn Off User Installed Windows Sidebar Gadgets” setting should be configured correctly	10586
105	“Maximum Log Size (KB)” should be configured correctly for the application/security/setup log	9603
106	“Turn Off Downloading of Game Information” setting should be configured correctly	1082

		8
107	“Turn off game updates” setting should be configured correctly	10850
108	“Prevent the computer from joining a homegroup” setting should be configured correctly	10183
109	The startup type of the NetMeeting Remote Desktop Sharing service should be correct	10763
110	“Do not allow passwords to be saved” setting should be configured correctly	10090
111	“Allow users to connect remotely using Remote Desktop Services” setting should be configured correctly	9985
112	“Always prompt for password upon connection” setting should be configured correctly	10103
113	The Remote Desktop Services “Set client connection encryption level” setting should be enabled	9764
114	“Set time limit for idle/disconnected sessions” policy should be set correctly for Terminal Services	10608
115	“Do not delete temp folder upon exit” setting should be configured correctly	10856
116	“Do not use temporary folders per session” setting should be configured correctly	9864
117	“Turn off downloading of enclosures” setting should be configured correctly	10730
118	“Allow indexing of encrypted files” setting should be configured correctly	10496
119	“Prevent indexing uncached Exchange folders” setting should be configured correctly	9866
120	“Prevent Windows Anytime Upgrade from running” setting should be configured correctly	10137
121	The Windows Error Reporting “Disable Logging” setting should be configured correctly	10157
122	“Windows Error Reporting” settings should be configured correctly	9914
123	“Turn off Data Execution Prevention for Explorer” setting should be configured correctly	9918
124	“Turn off Heap termination on corruption” setting should be configured correctly	9874
125	“Turn off shell protocol protected mode” setting should be configured correctly	10623
126	“Set Safe for Scripting” policy should be set correctly	9875

127	“Enable User Control Over Installs” policy should be set correctly	9876
128	“Prohibit non-administrators from applying vendor signed updates” setting should be configured correctly	9888
129	“Report Logon Server Not Available During User logon” setting should be configured correctly	9907
130	“Turn off the communication features” setting should be configured correctly	11252
131	“Turn off Windows Mail application” setting should be configured correctly	10882
132	“Prevent Windows Media DRM Internet Access” setting should be configured correctly	9908
133	“Disable Media Player for automatic updates” policy should be set correctly	10602
134	Automatic Updates should be enabled and features should be configured correctly	9403
135	The “Windows Media Center” features should be configured correctly	18300

3.10 Misconfigurations in Firewall Inbound Rules

S#	Issue	CCE
136	DHCP-In/DHCPV6-In Windows Firewall rules should be configured correctly	14986

3.11 Misconfigurations in Advanced Security

S#	Issue	CCE
137	“Log Dropped Packets” option for the Windows Firewall should be configured correctly	10502
138	“Log Successful Connections” option for the Windows Firewall should be configured correctly	10268
139	“Log File Path and Name” for the Windows Firewall should be configured correctly	10022
140	“Log File Size Limit” for the Windows Firewall should be configured correctly	9747
141	Display of a notification to the user when Windows Firewall blocks network activity should be enable	9774

142	“Windows Firewall: Apply local connection security rules” setting should be configured correctly	9329
143	“Windows Firewall: Apply local firewall rules” setting should be configured correctly	9686
144	Unicast response to multicast or broadcast requests should be enabled	9069
145	The Windows Firewall should be enabled	9465
146	Windows Firewall should allow or block inbound connections by default as appropriate	9620

3.13 Misconfigurations in Internet Explorer

S#	Issue	CCE
148	“Disable Configuring History” machine setting should be configured correctly	10387
149	"Disable changing Automatic Configuration settings" machine setting should be configured correctly	10638
150	"Make proxy settings per-machine (rather than per-user)" machine setting should be enabled	9870
151	"Prevent participation in the Customer Experience Improvement Program" machine setting should be configured correctly	10522
152	"Prevent performance of First Run Customize settings" machine setting should be configured correctly	10641
153	"Security Zones: Do not allow users to add/delete sites" machine setting should be enabled	10394
154	"Security Zones: Do not allow users to change policies" machine setting should be enabled	10037
155	"Security Zones: Use only machine settings" machine setting should be enabled	10096
156	"Turn off Crash Detection" machine setting should be configured correctly	10594
157	"Turn off Managing SmartScreen Filter" machine setting should be configured correctly	9973
158	"Turn off the Security Settings Check feature" machine setting should be configured correctly	10607
159	"Include updated Web site lists from Microsoft" machine setting should be configured correctly	10603
160	"Configure Delete Browsing History on exit" current user setting should be configured correctly	10590
161	"Prevent Deleting Web sites that the User has Visited" machine setting should be	1011

	configured correctly	0
1162	"Turn off InPrivate Browsing" machine setting should be configured correctly	9885
163	"Allow active content from CDs to run on user machines" machine setting should be disabled	10293
164	"Allow software to run or install even if the signature is invalid" machine setting should be disabled	10052
165	"Allow third-party browser extensions" machine setting should be configured correctly	9905
166	"Automatically check for Internet Explorer updates" machine setting should be configured correctly	10581
167	"Check for server certificate revocation" machine setting should be configured correctly	10074
168	"Check for signatures on downloaded programs" machine setting should be configured correctly	10055
169	"Intranet Sites: Include all network paths (UNCs)" machine setting should be configured correctly	9660
170	"Access data sources across domains" machine setting should be configured correctly for the Internet Zone	10380
171	"Allow cut, copy or paste operations from the clipboard via script" machine setting should be configured correctly for the Internet Zone	10002
172	"Allow drag and drop or copy and paste files" machine setting should be configured correctly for the Internet Zone	10033
173	"Allow font downloads" machine setting should be configured correctly for the Internet Zone	10403
174	"Allow installation of desktop items" machine setting should be configured correctly for the Internet Zone	9790
175	"Allow scripting of Internet Explorer web browser control" current user setting should be configured correctly for the Internet Zone	9779
176	"Allow script-initiated windows without size or position constraints" machine setting should be configured correctly for the Internet Zone	9882
177	"Allow Scriptlets" machine setting should be configured correctly for the Internet Zone	10685
178	"Automatic prompting for file downloads" machine setting should be configured correctly for the Internet Zone	10389
179	"Download signed ActiveX controls" machine setting should be configured correctly for the Internet Zone	9917
180	"Download unsigned ActiveX controls" machine setting should be configured correctly for the Internet Zone	10433

181	"Include local directory path when uploading files to a server" machine setting should be configured correctly for the Internet Zone	10646
182	"Initialize and script ActiveX controls not marked as safe" machine setting should be configured correctly for the Internet Zone	10561
183	"Java permissions" machine setting should be configured correctly for the Internet Zone	10182
184	"Launching applications and files in an IFRAME" machine setting should be configured correctly for the Internet Zone	9821
185	"Launching programs and unsafe files" machine setting should be configured correctly for the Internet Zone	10650
186	"Logon options" machine setting should be configured correctly for the Internet Zone	10472
187	"Loose XAML files" machine setting should be configured correctly for the Internet Zone	10672
188	"Only allow approved domains to use ActiveX controls without prompt" machine setting should be configured correctly for the Internet Zone	9793
189	"Open files based on content, not file extension" machine setting should be configured correctly for the Internet Zone	10107
190	"Run .NET Framework-reliant components signed with Authenticode" machine setting should be configured correctly for the Internet Zone	10515
191	"Run .NET Framework-reliant components not signed with Authenticode" machine setting should be configured correctly for the Internet Zone	10625
192	"Software channel permissions" machine setting should be configured correctly for the Internet Zone	10425
193	"Turn Off First-Run Opt-In" machine setting should be configured correctly for the Internet Zone	10434
194	"Turn on Cross-Site Scripting (XSS) Filter" machine setting should be configured correctly for the Internet Zone	10276
195	"Turn on Protected Mode" machine setting should be configured correctly for the Internet Zone	10676
196	"Use Pop-up Blocker" machine setting should be configured correctly for the Internet Zone	10486
197	"Userdata persistence" machine setting should be configured correctly for the Internet Zone	10200
198	"Web sites in less privileged Web content zones can navigate into this zone" machine setting should be configured correctly for the Internet Zone	10622
19	"Java permissions" machine setting should be configured correctly for the Intranet Zone	10566

100	"Java permissions" machine setting should be configured correctly for the Local Machine Zone	10319
101	"Download signed ActiveX controls" machine setting should be configured correctly for the Locked-Down Internet Zone	10095
102	"Java permissions" machine setting should be configured correctly for the Locked-Down Internet Zone	10597
103	"Java permissions" machine setting should be configured correctly for the Locked-Down Intranet Zone	10342
104	"Java permissions" machine setting should be configured correctly for the Locked-Down Local Machine Zone	10535
105	"Java permissions" machine setting should be configured correctly for the Locked-Down Restricted Sites Zone.	10275
106	"Java permissions" machine setting should be configured correctly for the Locked-Down Trusted Sites Zone	10654
107	"Access data sources across domains" machine setting should be configured correctly for the Restricted Sites Zone	10525
108	"Allow active scripting" machine setting should be configured correctly for the Restricted Sites Zone	10393
109	"Allow binary and script behaviors" machine setting should be configured correctly for the Restricted Sites Zone	10547
110	"Allow cut, copy or paste operations from the clipboard via script" machine setting should be configured correctly for the Restricted Sites Zone	10539
111	"Allow drag and drop or copy and paste files" machine setting should be configured correctly for the Restricted Sites Zone	9667
112	"Allow file downloads" machine setting should be configured correctly for the Restricted Sites Zone	10466
113	"Allow font downloads" machine setting should be configured correctly for the Restricted Sites Zone	9982
114	"Allow installation of desktop items" machine setting should be configured correctly for the Restricted Sites Zone	10475
115	"Allow scripting of Internet Explorer web browser control" current user setting should be configured correctly for the Restricted Sites Zone	10725
116	"Allow META REFRESH" machine setting should be configured correctly for the Restricted Sites Zone	10664
117	"Allow script-initiated windows without size or position constraints" machine setting should be configured correctly for the Restricted Sites Zone	9814
118	"Allow Scriptlets" machine setting should be configured correctly for the Restricted Sites Zone	10630

119	"Allow status bar updates via script" machine setting should be configured correctly for the Restricted Sites Zone	10431
120	"Automatic prompting for file downloads" machine setting should be configured correctly for the Restricted Sites Zone	9959
121	"Download signed ActiveX controls" machine setting should be configured correctly for the Restricted Sites Zone	10470
122	"Download unsigned ActiveX controls" machine setting should be configured correctly for the Restricted Sites Zone	10461
123	"Include local directory path when uploading files to a server" machine setting should be configured correctly for the Restricted Sites Zone	9781
124	"Initialize and script ActiveX controls not marked as safe" machine setting should be configured correctly for the Restricted Sites Zone	10347
125	"Java permissions" machine setting should be configured correctly for the Restricted Sites Zone	10620
126	"Launching applications and files in an IFRAME" machine setting should be configured correctly for the Restricted Sites Zone	10360
127	"Launching programs and unsafe files" machine setting should be configured correctly for the Restricted Sites Zone	10744
128	"Logon options" machine setting should be configured correctly for the Restricted Sites Zone	10651
129	"Loose XAML files" machine setting should be configured correctly for the Restricted Sites Zone	10178
130	"Navigate windows and frames across different domains" machine setting should be configured correctly for the Restricted Sites Zone	10642
131	"Only allow approved domains to use ActiveX controls without prompt" machine setting should be configured correctly for the Restricted Sites Zone	9832
132	"Open files based on content, not file extension" machine setting should be configured correctly for the Restricted Sites Zone	10277
133	"Run .NET Framework-reliant components not signed with Authenticode" machine setting should be configured correctly for the Restricted Sites Zone	9898
134	"Run .NET Framework-reliant components signed with Authenticode" machine setting should be configured correctly for the Restricted Sites Zone	9673
135	"Run ActiveX controls and plugins" machine setting should be configured correctly for the Restricted Sites Zone	9792
136	"Script ActiveX controls marked safe for scripting" machine setting should be configured correctly for the Restricted Sites Zone	10554
137	"Scripting of Java applets" machine setting should be configured correctly for the Restricted Sites Zone	10083

138	"Software channel permissions" machine setting should be configured correctly for the Restricted Sites Zone	9669
139	"Turn Off First-Run Opt-In" machine setting should be configured correctly for the Restricted Sites Zone	10420
140	"Turn on Cross-Site Scripting (XSS) Filter" machine setting should be configured correctly for the Restricted Sites Zone	10105
141	"Turn on Protected Mode" machine setting should be configured correctly for the Restricted Sites Zone	9945
142	"Use Pop-up Blocker" machine setting should be configured correctly for the Restricted Sites Zone	10094
143	"Userdata persistence" machine setting should be configured correctly for the Restricted Sites Zone	9760
144	"Web sites in less privileged Web content zones can navigate into this zone" machine setting should be configured correctly for the Restricted Sites Zone	10609
145	"Java permissions" machine setting should be configured correctly for the Trusted Sites Zone	10696
146	"Turn off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools" machine setting should be configured correctly	10595
147	"Turn off configuring the update check interval (in days)" machine setting should be configured correctly	9776
148	"Consistent Mime Handling: Internet Explorer Processes" machine setting should be configured correctly	10138
149	"Mime Sniffing Safety Feature: Internet Explorer Processes" machine setting should be configured correctly	10635
151	"MK Protocol Security Restriction: Internet Explorer Processes" machine setting should be configured correctly	10265
152	"Protection From Zone Elevation: Internet Explorer Processes" machine setting should be configured correctly	10574
153	"Restrict ActiveX Install: Internet Explorer Processes" machine setting should be configured correctly	10405
154	"Restrict File Download: Internet Explorer Processes" machine setting should be configured correctly	10578
155	"Scripted Window Security Restrictions: Internet Explorer Processes" machine setting should be configured correctly	10604

4. Mac OS X Configuration Assessment

Tool Used: **Lynis**

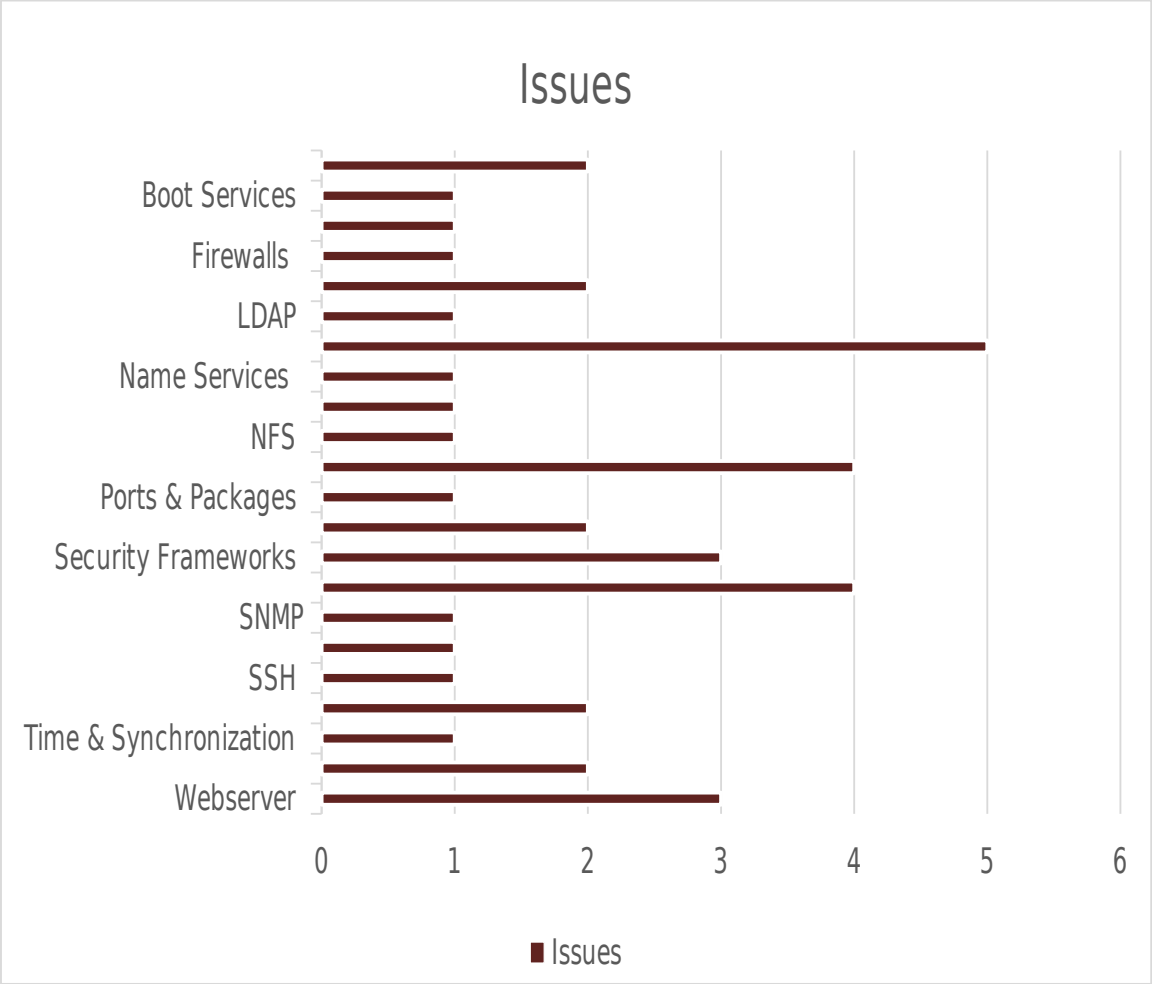
Version: **2.5.5**

Type of Scan: **Privileged**

Target Operating System: **10.12.5**

Kernel Version: **16.6.0**

Hardware Platform: **64 bit**



4.1 Misconfigurations in PHP

#	Issue	Description	How to solve	Additional resources
1	PHP expose_php option	PHP option expose_php is turned on, which can reveal useful information for attackers	Change the expose_php line to: expose_php = Off	http://php.net/manual/en/security.php
2	PHP allow_url_fopen	PHP allows file downloads with the allow_url_fopen setting so the option should be disabled if it is not strictly needed for the applications running on the server	Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP	http://php.net/manual/en/security.php
3	PHP Suhosin extension status	Suhosin is absent	Harden PHP by enabling suhosin extension and deactivating suhosin simulation mode	

4.2 Misconfiguration in File Integrity

#	Issue	Description	How to solve	Additional

				resources
4	Inadequate separation of partitions	Partitions like /tmp, /home, /var can be easily filled by users of a system when not being separated from the root file system, increasing the risk of cause malfunctioning to other system components	Symlinked mount point needs to be checked manually and /home, /tmp, /var need to be placed on a separated partition	N/A

4.3 Misconfiguration in Hardening

#	Issue	Description	How to solve	Additional resources
5	Inappropriate permissions on installed compilers	Due to protections in the Linux kernel, memory allocation and execution of processes, is limited. To circumvent these protections, a compiler on the related system is needed, so the attacker can determine specific memory locations and leverage a so-called exploit. Execution of the compiler found is not currently limited to authorized users	Remove unneeded compilers to prevent users from compiling source code into binary programs or if needed on the system, change file permissions to ensure that only the root can use the compiler	https://linux-audit.com/understanding-linux-privilege-escalation-and-defending-against-it/ https://linux-audit.com/audit-installed-compilers-and-their-packages/
6	Absence of malware scanner	Lack of malware scanner to search for traces of malware. Regular checks are advised to improve the detection rate, to prevent the intrusion of the system and malware from spreading to other systems	Harden the system by installing ClamAV for generic virus detection and one of Rootkit Hunter or Chkrootkit or OSSEC for rootkit detection	https://gist.github.com/zhurui1008/4fdc875e557014c3a34e

4.4 Misconfiguration in Web Settings

#	Issue	Description	How to solve	Additional resources
7	Missing PAM module	Lack of adequate password protection and strengthening. On Unix based systems this is usually done via PAM modules and related configuration files	Install a PAM module like pam_cracklib or pam_passwdqc for password strength testing	http://www.techrepublic.com/article/enforce-strong-passwords-with-pam-passwdqc/

4.5 Misconfiguration in Name Resolution

#	Issue	Description	How to solve	Additional resources
7	Missing Name Resolution	N/A	Add the IP name and FQDN to /etc/hosts for proper name resolving	http://www.inmotionhosting.com/support/website/how-to/how-to-edit-your-hosts-file-on-a-mac

4.6 Misconfiguration in Logging

#	Issue	Description	How to solve	Additional resources
	Deleted file in use	Deleted file is in use by application. This may indicate malicious software is trying hide its presence on the system..	Investigate what deleted files are in use and why and determine which application keeps them open and any related reasons	https://cisofy.com/controls/LOGG-2190/

4.7 Misconfiguration in Network Time Protocol

#	Issue	Description	How to solve	Additional resources
	NTP mismatch	Difference exists between active configuration and the one stored on disk and can result in a non-	Check both the output of ntpq and the nodes stored in the	https://arstechnica.com/civis/

	functional NTP configuration after reboot.	configuration. Adjust any differences where appropriate.	viewtopic.php?t=34734

4.8 Misconfiguration in Package Auditing

#	Issue	Description	How to solve	Additional resources
	Missing package audit tool	No tool included to check for security packages, to fix vulnerable versions of installed software	Install a package audit tool to determine vulnerable packages	https://linux-audit.com/perform-netbsd-security-audit-with-pkg_admin/

4.9 Misconfiguration in Automation Management

#	Issue	Description	How to solve	Additional resources
	No automation tools for system management	No tools installed to help automating system management. This decreases integrity and stability of systems, as systems are not equally managed and configured leaving major exceptions	Install and configure Puppet automation tool for configuration management, to help repeat tasks and increase integrity of systems	https://puppet.com

4.10 Misconfiguration in Firewall

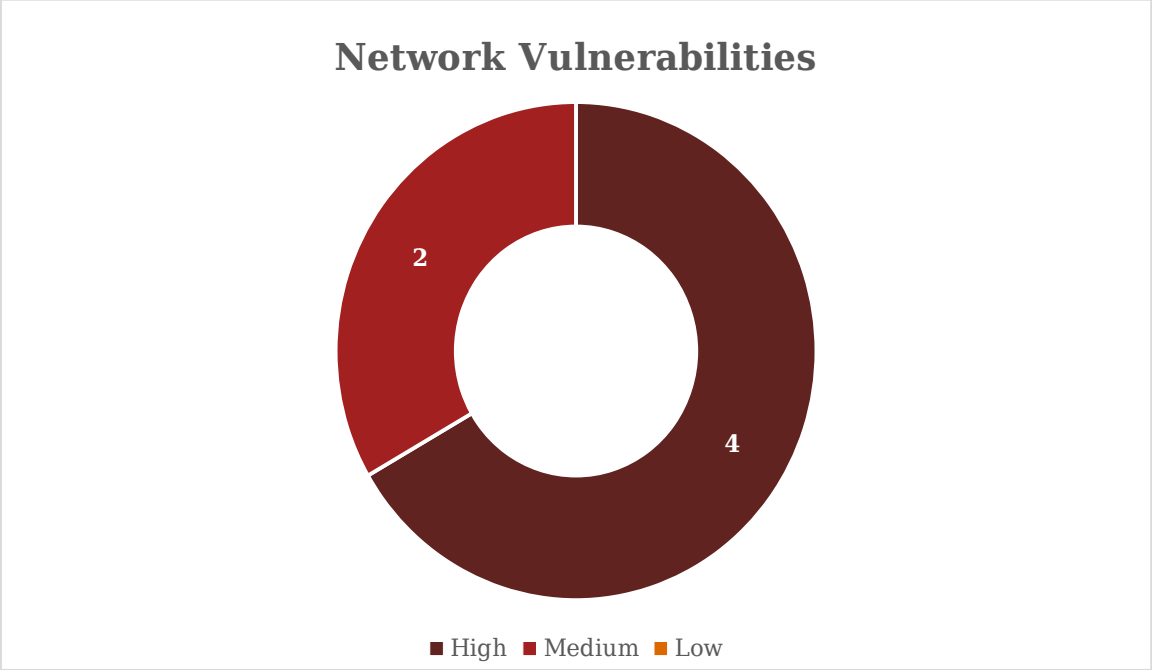
#	Issue	Description	How to solve	Additional resources
7	Lack of firewall	Depending on the type of system and sensitivity of the data being stored and processed, a firewall is advised, currently not in place	Configure a firewall to filter incoming and outgoing packet traffic	https://www.macobserver.com/tips/how-to/macos-sierra-firewall-stealth-mode/

4.11 Misconfiguration in Postfix Hardening

#	Issue	Description	How to solve	Additional resources
7	VRFY command	VRFY command has not been disabled to protect user's information from being exposed by SMTP server. Currently an attacker can verify the valid user ID locally on sendmail via port 25	Disable the 'VRFY' command by running run pos**onf -e disable_vrfy_command=yes to change the value disable_vrfy_command=no	https://social.technet.microsoft.com/Forums/ie/en-US/acb6e8e8-795e-4f8c-9785-f237b948a626/what-is-vrfy-command-and-how-disable-its-functionality-to-protect-users-

information-to-be-expose-by?forum=exchangesvrclients

5. Network Security Assessment – Office network



5.1 Absence of SIEM solution

Score:

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Description

During the review of network architecture, it was noted that J**** management have not implemented a monitoring solution to monitor internal and external threats to J****. Moreover, security events generated from systems like servers, network devices and end users' machines are not stored and interpreted centrally to allow management to take defensive action more quickly against threats.

Impact

In the absence of a monitoring solution, management will not be able to proactively block intrusion attempts from known and unknown sources. This will allow attackers to intrude and deploy malicious files and construct backdoors, to obtain sensitive J**** information without any resistance. Management may not be aware of any ongoing attacks against the infrastructure.

Recommendation

1. **Interim Action:** Review periodically (e.g. daily) the current system and security logs available from the infrastructure implemented.
2. **Short Term**: Centralize the security logs in a platform (log management or SIEM platform) to support and accelerate the analysis of security events.
3. **Medium Term:** Implement a SIEM solution and derive and prioritize a comprehensive set of security information feeds for SIEM's central processing engine, including syslog events of infrastructure devices, application systems and environmental feeds.
4. **Long Term (Optimum):** Integrate network components to be monitored and profiled, one at a time.
5. **Long Term (Most Secure):** Optimize SIEM alert thresholds to suppress false-positives. Engage vendor in on-site training of J**** resources to increase in-house expertise.

References

http://searchsecurity.techtarget.com/tip/SIEM-best-practices-for-advanced-attack-detection

http://www.computerweekly.com/feature/Genpact-boosts-security-management-with-SIEM-tool

5.2 Absence of security solutions to monitor threats

Score:

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Description

During the review of network architecture, we have observed that J**** has not implemented solutions to proactively detect and protect the network from internal and external threats. Currently, there are missing solutions in place to detect and actively prevent threats. For e.g.

- IPS/IDS
- Advanced Persistent Threat (APT) solution
- Secure Email Gateway
- Network Anti-Malware

In order to validate this scenario we carried out the test by uploading a malicious file that checks network connection on the server. We observed that there are no controls are implemented over the network to analyze and detect malicious file entering the network as we were able to successfully upload malicious file "eicarcom2" from internet (non-whitelisted IP address) suggesting that appropriate network level security controls are also not implemented.

***eicarcom2** is a known malicious file designed to test effectiveness of controls and is safe for testing*

Impact

In the absence of security solutions, it becomes easier for an attacker to compromise the network through weaknesses in the infrastructure and/or social engineering attacks. This often results in having malware and backdoors implanted in critical infrastructure to act as a malicious gateway to the infrastructure without detection over long periods of time.

Recommendation

1. **Medium Term:** Evaluate email security gateway and intrusion prevention system vendors. Evaluate implementation formats that is optimal for J****'s environment. Consider whether to choose a public cloud-based, hybrid public/private cloud-based, on-premise hardware-based, virtual on-premise appliance-based or email server-based solution.

2. **Long Term:** Engage in project-based implementation with vendor to implement chosen security solutions.

Screenshot

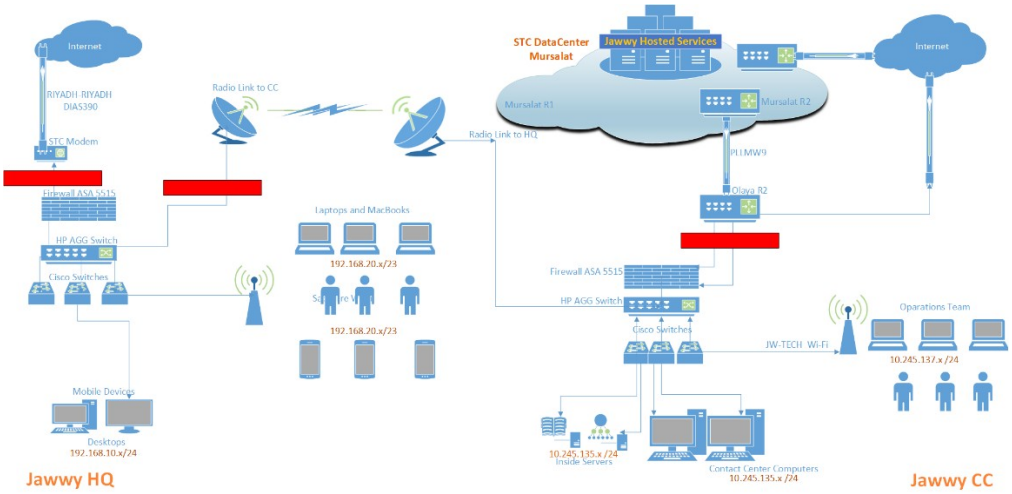


Figure 1

Figure 1: Shows the conceptual network topology and the critical network gateway points where security solutions should be deployed as

References

https://www.gartner.com/reviews/market/intrusion-prevention-system

http://searchsecurity.techtarget.com/feature/Comparing-the-best-intrusion-prevention-systems

http://searchsecurity.techtarget.com/feature/Comparing-the-best-email-security-gateways

Critica Hig Medium Low Info

5.3 Absence of user segregation over network

Score:

Description

Based on our understanding of the existing network segment for users across J****, we understand that, four VLANs are created in HQ using separate the following IP subnets:

- 192.168.10.0/24
- 192.168.20.0/23
- 192.168.30.0/24
- 192.168.40.0/24

However, during the review of the firewall configuration, it was clear that J**** HQ have a flat network where generic rules have been created for VLANs. The ruleset does not restrict visibility of systems/machines from one VLAN to another and this was confirmed by the unrestricted ability to send and successfully receive ICMP echo request packets to machines on different subnets while being connected to S*******'s wireless network.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	Low
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Impact

In the absence of appropriate network level segregation, a user with malicious intent can traverse across network segments and gain unauthorized access to critical J**** systems, potentially extracting personnel, corporate, email communication and/or confidential trade information.

Recommendation

1. **Short Term:** Access to sensitive systems like LDAP server should be restricted to administrative users only
2. **Medium Term:** Adequate network level segregation should be implemented to restrict user access to specific domains based on the user needs and the service requirements fulfilled.

Screenshot

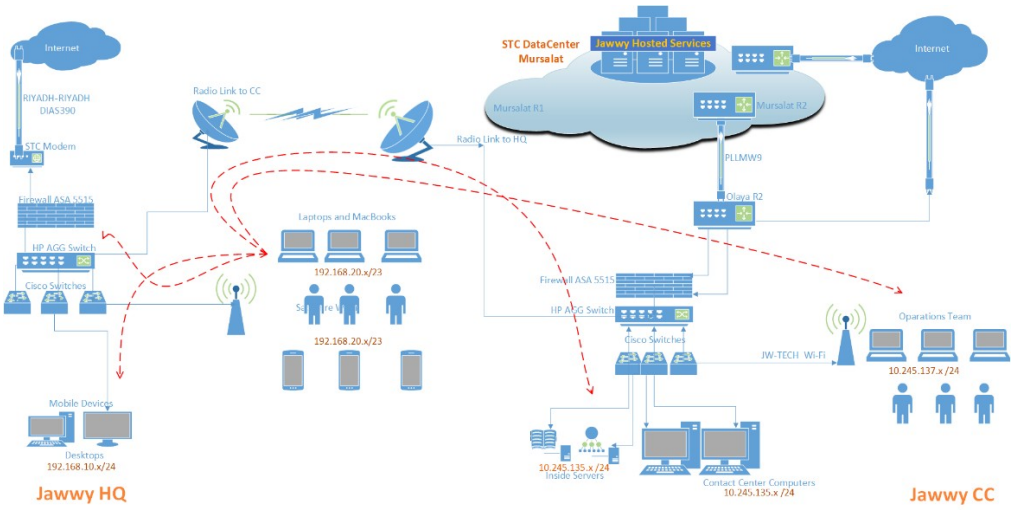


Figure 1: Shows the conceptual network topology at J**** which allows inter-VLAN visibility and network

Figure 1

References

http://searchsecurity.techtarget.com/WLAN-security-Best-practices-for-wireless-network-security

5.4 Open Connectivity to CC server room using LAN net

Score:

Description

During the review of network architecture, it was noted that any end user at J**** can connect to the LAN network via Ethernet and access servers in the data center located in the Contact Center. There is currently no network level security feature or authentication requirements to restrict access to authorized users.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Impact

A malicious user may connect their machines via LAN and attempt to connect to servers in the contact center to extract sensitive information. Similarly, a legitimate user might connect their infected endpoint unknowingly to the CC server room and have worms traverse across networks.

Recommendation

1. **Interim Action:** MAC binding should be implemented to prevent attackers from spoofing their identity

2. **Short Term:** User machines must be scanned and have malware cleaned against updated database definitions to ensure servers are not compromised

3. a) **Medium Term:** Network Level Authentication must be enabled to restrict network access to legitimate users on a 'Principle of Least Privilege' basis

   b) **Long Term (Optimum):** Implement a dedicated Network Access Control solution

Screenshot

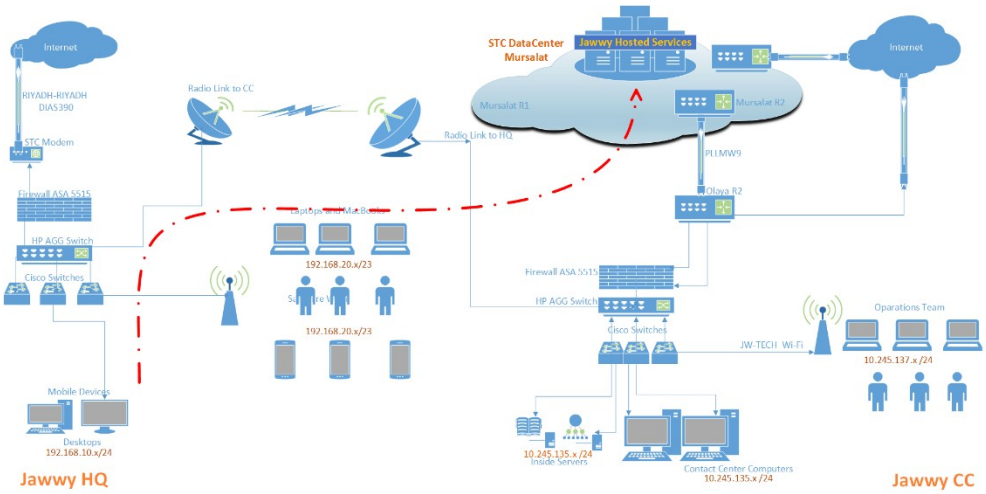


Figure 1: Shows the conceptual network topology at J**** which allows machines unrestricted network traversal from J****-HQ to J**** CC over

5.5 Lack of protection around UPS

Score:

Description

S*******'s Uninterruptible Power Supply system does not have requisite protection. The UPS room has open access and the cabinet containing the UPS remains unlocked. An attacker can gain access to the UPS system by entering the room undetected, gain administrative privileges on the UPS unit's management console and maliciously tamper with relay configurations to prevent important alarms from triggering or the UPS from activating when required. The attacker can then proceed to register the UPS on J****'s unsegmented network via up Ethernet and set up a backdoor via USB to access remotely.

Environmental Score	
Attack vector	Physical
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Impact

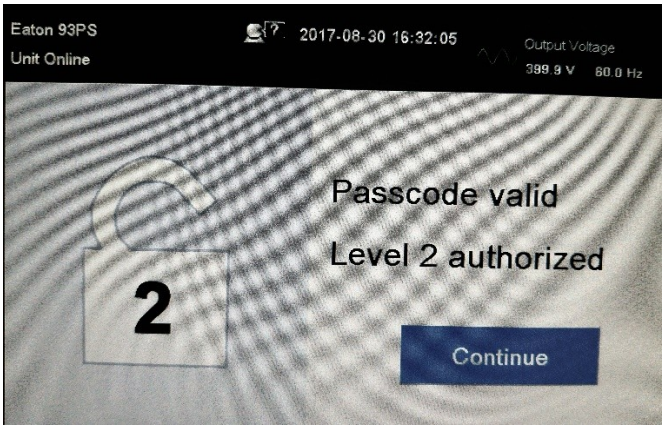
An advanced attacker with adequate resources can exploit flaws in the firmware to cause a power failure and cause a major denial of service when the UPS is required for an electrical supply. This is compounded by the fact that there is only one UPS at S*******.

Moreover it has been theorized that the UPS could be made to overcharge its batteries and generate, flammable hydrogen if enough firmware fail safes are compromised, to cause combustion. This is a great risk at J****, as the UPS is located within the office instead of being on a separate 'technical area' level.

Recommendation

1. **Interim Action:** Change default Level 2 and Level 3 Passcodes.
2. **Short Term:** Secure UPS room and Lock cabinet containing UPS.
3. **Medium Term:** Implement a network inventory tool that automatically scans the network against a preconfigured inventory of trusted assets to keep track of changes to the infrastructure landscape and prevent an attacker from an unauthorized network deployment of the UPS console.
4. **Long Term (Optimum):** Integrate UPS into SIEM solution for dedicated threat monitoring by the SOC function
5. **Long Term (Most Secure):** Add multiple UPS systems and migrate them to a different dedicated technical floor

Screenshot



References

http://www.pcworld.com/article/236875/batteries_go_boom.html

Critical | High | **Medium** | Low | Info

5.6 Inadequate content filtering and bandwidth manage

Score: 

Description

During our review of J****'s network architecture, it was noted that content or bandwidth usage is not restricted for individual users over the internet. Users have unrestricted access to the internet and can browse, download and/or upload most material to/from the internet.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Impact

In the absence of content filtering and bandwidth management, users might intentionally or unintentionally download malicious content from unsecure sources, such as torrents and other untrusted platforms. This may allow attackers to target J**** employees to divert them to untrusted websites to eventually gain access to sensitive credentials or create backdoors to the J**** network. Moreover, critical business services requiring internet connectivity might be affected due unavailability of adequate bandwidth.

Recommendation

1. **Interim Action:** Draw an awareness campaign around internet usage policy to remind employees about appropriate internet browsing activity

2. a) **Short Term:** Establish content filtering for external internet connectivity to restrict access to gaming content, anti-government rhetoric, social media, and black hat activities. Additional access should only be whitelisted on a need-to-have basis, as authorized and justified by J****'s requirements.

   b) **Medium Term:** Implement a solution to assess J****'s traffic profile by analyzing network traffic to identify when and how bandwidth is being consumed, by whom and by what applications.

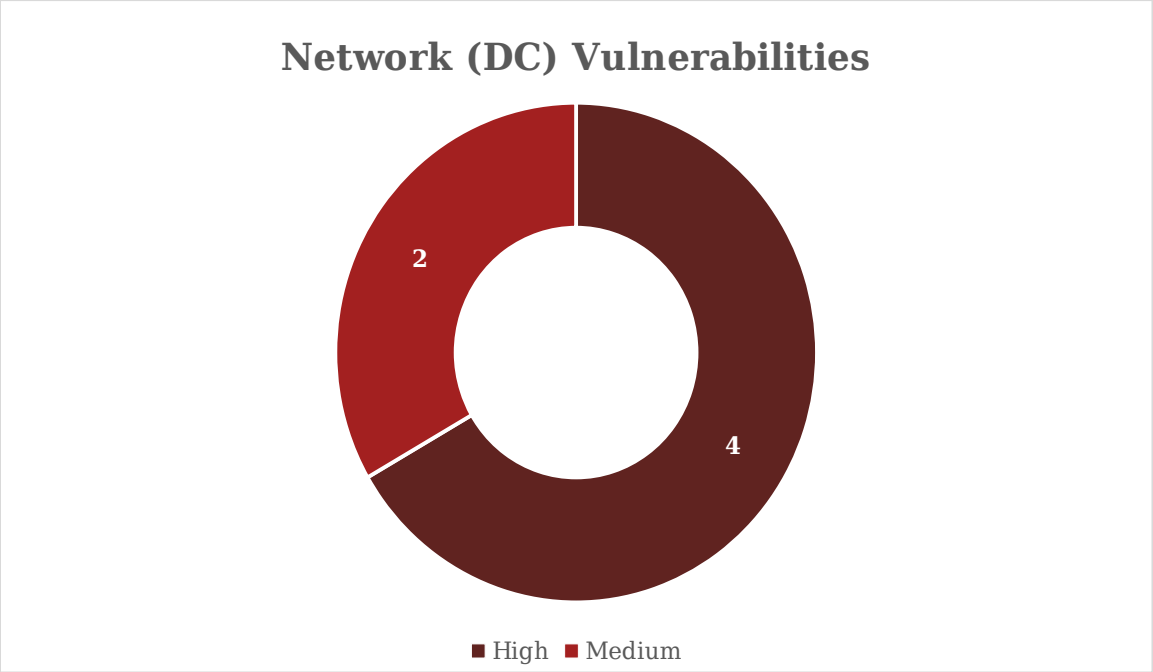
3. **Long Term (Optimum):** Establish and monitor quality of service (QoS) policies to ensure that business-critical traffic takes priority over nonessential traffic and ensure data links always have access to adequate bandwidth for sensitive services.

4. **Long Term (Most Secure):** Optimize WAN acceleration to optimize the usage of WAN links and direct business-critical traffic such as administrative access, J****'s rich media content services across one link while sending the less essential employee traffic across another.

References

http://www.apmdigest.com/5-best-practices-for-network-bandwidth-management

6. Network Security Assessment – Data Center



6.1 Public-Facing Jump-Servers used internally

Environmental Score	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Unproven
Remediation level	Official fix
Report confidence	Confirmed

Description

During the review of J****'s network architecture, it was noted that administrative users use terminal servers published over the internet in the demilitarized zone to access sensitive applications in the data center VLAN, without having additional security measures like encryption and secure authentication in place.

Impact

An attacker may attempt to compromise the publicly available servers by using several methods such as brute forcing, exploiting unpatched Linux/Windows vulnerabilities to gain access to J****'s internal network. The attacker can then obtain sensitive J**** information or disrupt normal business operations.

Recommendation

1. **Interim Action:** Terminal servers should be secured by using non-default ports usage
2. **Short Term**: Implement a client-based VPN solution to connect to internal servers through secure encrypted channels
3. **Medium Term:** Enforce complex password management and two-factor authentication for setting up VPN tunnel

Screenshot

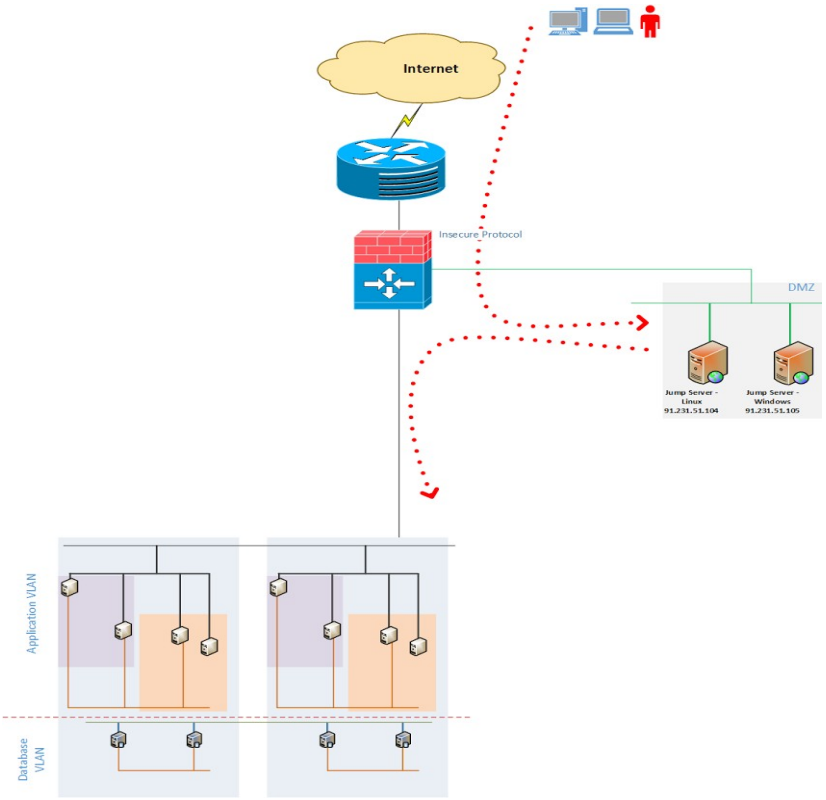


Figure 1: Shows the conceptual network topology where the publicly exposed DMZ jump servers are directly utilized to access sensitive applications on the

Figure 1

References

https://security.stackexchange.com/questions/34000/is-there-a-secure-way-to-have-a-publicly-facing-terminal-server

6.2 Lack of database encryption

Score: 8.0

Description

S******* has hosted most of the application and database servers in STC's environment. During our understanding meeting with STC personnel, it was noted that S******* has not enabled encryption on any of the application databases.

Impact

Without encryption, sensitive customer and company information can be viewed by anyone accessing the server. This information might be stolen or misused by employees or vendors. Additionally, in case of any attacks the information shall be openly available to attackers. This can lead to the breach of critical client data and result to the potential loss of customer confidence, litigation concerns, and bad press.

Recommendation

Short Term: It is recommended that S******* follows a defense in depth approach and enable database encryption.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	Low
Temporal Score	
Exploit maturity	High
Remediation level	Official fix
Report confidence	Confirmed

Affected Targets
All application
Databases

References

http://searchsecurity.techtarget.com/tip/The-ins-and-outs-of-database-encryption

6.3 Lack of AWS cloud security services purchases

Score:

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Description

S******* has placed its critical J**** customer portal servers in AWS cloud. AWS has provided a portal to allow S******* to connect to their servers. As per our understanding of AWS cloud services, S******* has not purchased any supplemental security services form AWS such as following:

- web application firewall,
- IPS,
- Database encryption,
- Host based Intrusion Prevention Solution,
- Antivirus,
- Etc.

Impact

Any attack on J**** applications may not be prevented by AWS. It is possible that J**** applications are exploited which would drastically effect customers and pose a risk to S******* reputation.

Recommendation

1) Interim Action: Purchase security features from AWS cloud to immediately secure S******* servers
2) **Short Term:** All access to service interfaces should be constrained to authenticated and authorized individuals
3) Medium Term: Applications should be designed and developed with secure coding practices to identify and mitigate threats to their security. Those that are vulnerable to security issues which could compromise S******* data, cause loss of service or enable other malicious activity should be decommissioned

References

https://www.excella.com/insights/5-ways-to-secure-your-aws-environment

https://www.infoworld.com/article/3026395/security/how-to-secure-amazon-web-services-like-a-boss.html

6.4 Absence of Web Application Firewall

Score:

Description

During the review of network architecture, we have observed that J**** has not implemented web application firewall to proactively detect and protect the applications from internal and external application level threats.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Impact

In the absence of web application firewall S******* may not be capable to detect and block attacks targeting application exposed to the internet which may result in loss or theft of sensitive customer or company information.

Recommendation

It is recommended that web application firewall is implemented which would block attacks targeted on websites, web-based applications, as well as the web server infrastructure.

6.5 Lack of Host-based intrusion prevention system

Score:

Description

During our understanding meeting with STC personnel we noted that although STC has secured S******* servers with network level controls, minimal security has been implemented over the server level. For instance, we noted that no Host-based Intrusion Prevention System has been implemented by S*******.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Impact

In the absence of a HIPS solution, a plethora of advanced attacks on the server may go unnoticed which may allow the attacker to destroy or extract sensitive information resulting in financial and/or reputational loss.

Recommendation

Short Term: It is recommended to enable windows firewall and similarly Iptables firewall on Linux environment

Medium Term: HIPS solution from an established vendor should be implemented to detect the attack signatures and prevent ongoing attacks using a database of signatures.

Long Term: HIPS solution should be fine-tuned to enable following:

- File integrity monitoring
- Behavior/anomaly based

References

https://www.lifewire.com/host-based-intrusion-prevention-2486685

6.6 Blanket use of site-to-site VPN tunneling

Score:

Description

J**** have configured a site-to-site VPN solution with a third-party vendor which is risky. Typically, such a setup is only necessary where both environments have multiple systems that need to access and talk to each other continuously, whereby a site-to-site VPN creates one big network between the two companies. In S*******'s current situation a user-based VPN would be more appropriate.

Environmental Score	
Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None
Temporal Score	
Exploit maturity	Functional
Remediation level	Official fix
Report confidence	Confirmed

Impact

Site-to-site VPN effectively extends the security perimeter to the third-party's network, so
there is little to no visibility over someone accessing something they shouldn't at the third-party site, or over a worm traversing from the third-party network to J****'s network.

Recommendation

1. a) **Medium Term:** If site-to-site VPN is required, limit access to only resources that need it and not the entire network by creating a VLAN in which all servers that the third-party needs, reside

   b) **Long Term (Optimum):** Setup user-based VPN on a per use basis with specific Active Directory credentials that restrict what the account can access in the network and with additional time limits

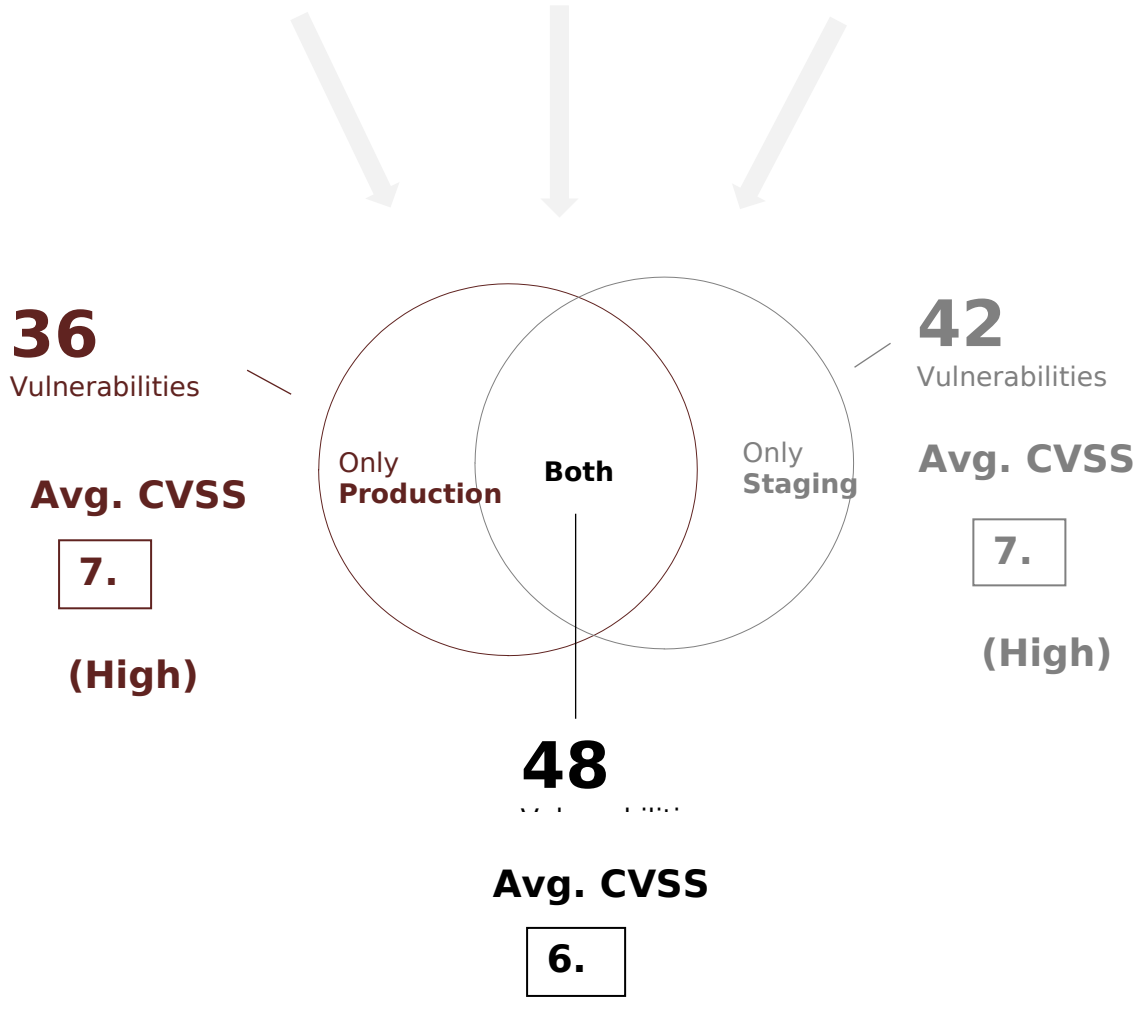
References

http://searchmidmarketsecurity.techtarget.com/tip/IPsec-tunneling-Exploring-the-security-risks

7. Internal Vulnerability Assessment

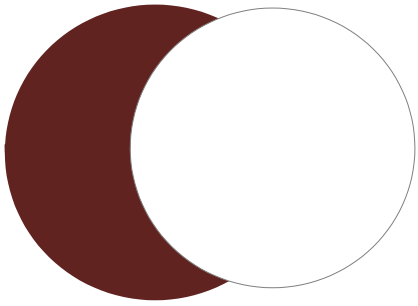
30 Applications Tested | 156 IP Addresses Scanned

ADM	HP QA Testing Tools	Oracle OAM Test Server
Avaya	IVR	ResponseTek
Tableau	JON / NTP	RMS
ETL Dev / STG	MGM	SAP HANA
ETL Test	ODC SME	Satellite
DMZ Rev Proxy	ODS	SSO Testing
Egain	ODS Jump Server	STG REV PROXY
ESB	OMS App Testing	Sugar CRM
File Server	OMS DB Testing	SVN / GIT
Git/Nexus	OMS Tomcat Worker	Syslog



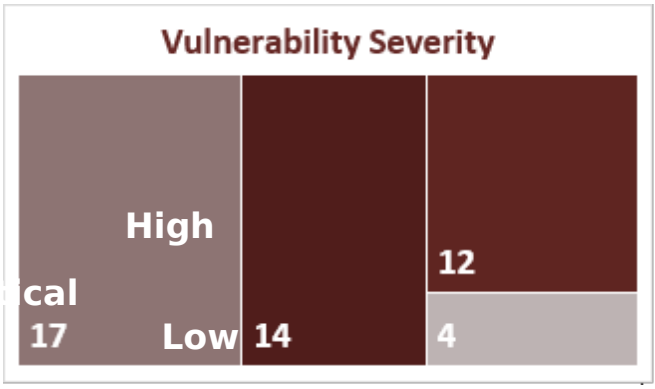
(Medium)

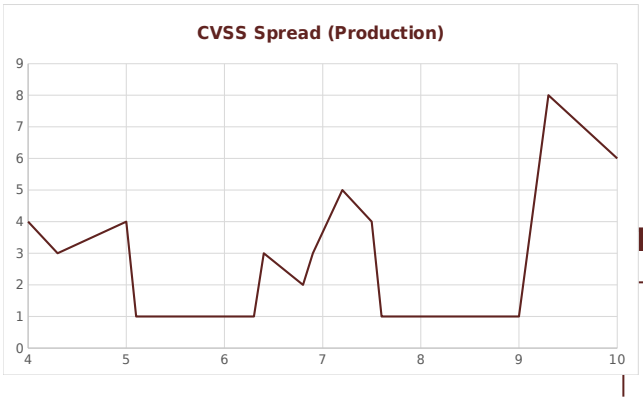
Credentialed
Non-privileged
82% 17 %



Only Production (36/126)

[This Tree Map helps visualize the breakdown of vulnerabilities in servers that are only in the Production environment by severity. The objective is to put into perspective the approximate ratio of critical to non-critical





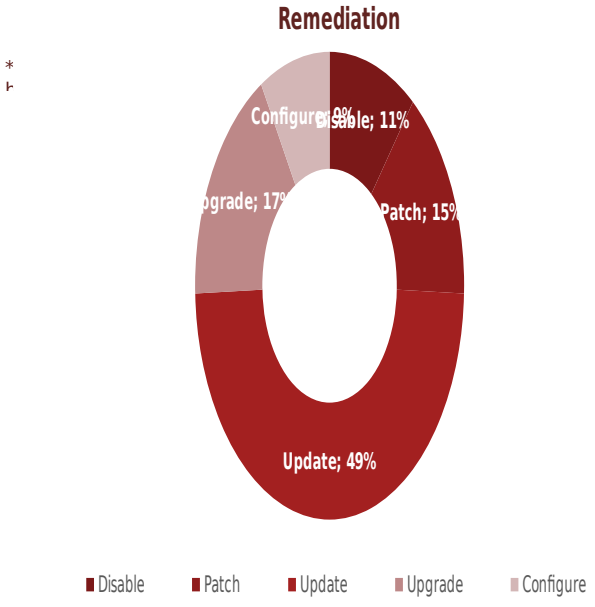
Top Risks

1. **Outdated Open SSL version**
2. **Outdated EMC Networker**
3. **Outdated CentOS version**

of Vulnerabilities

[This Scatter Graph helps visualize the breakdown of vulnerabilities by CVSS. The objective is to be able find clusters that indicate where most vulnerabilities lie. For example, we can see that there are a lot of vulnerabilities between 9.0 – 9.5 but not many between 5.0 – 6.0]

CVSS Score

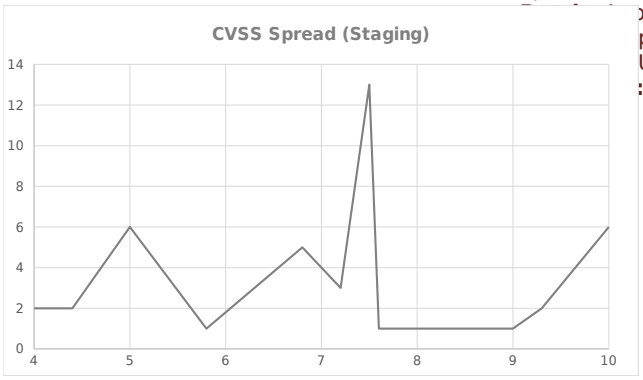


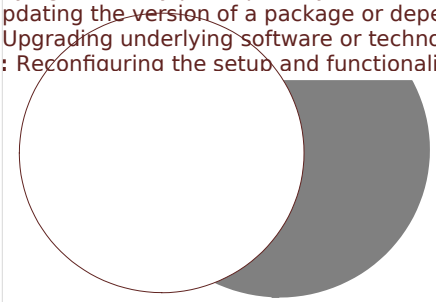
Prod.xls

[This Pie Chart helps visualize the breakdown of remedial actions by category. The objective is to put into perspective the effort (time and resources) required to close the vulnerabilities. For example, a vulnerability which requires structural reconfiguration in the way it is setup (i.e. workflow, permissions) will require significantly more effort to fix, than a vulnerability that simply requires a pre-existing patch, already released by the vendor, to be simply applied]

Credentialed
Non-privileged
95% 5 %

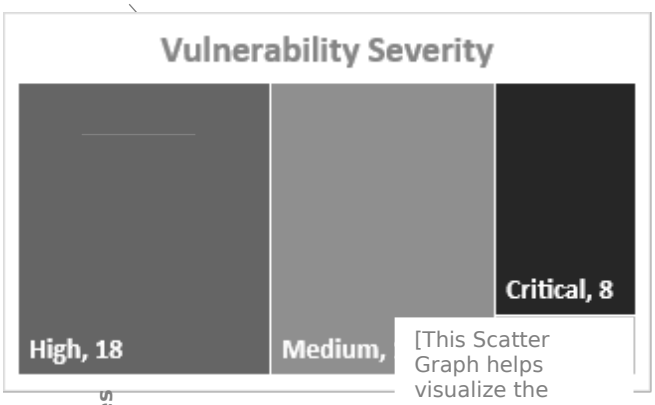
Disable: Removing a functionality, service or technology option
plying a security patch publicly released by vendor
pdating the version of a package or dependency
Upgrading underlying software or technology
: Reconfiguring the setup and functionality





(42/126) Only Staging

[This Tree Map helps visualize the breakdown of vulnerabilities in servers that are only in the Staging environment by severity. The objective is to put into perspective the approximate ratio of critical to non-critical flaws, so remedial action can be budgeted for and prioritized accordingly]

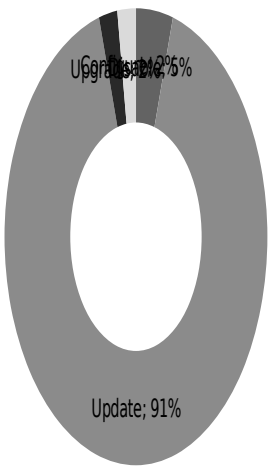


[This Scatter Graph helps visualize the breakdown of vulnerabilities by CVSS. The objective is to be able find clusters that indicate where most vulnerabilities lie. For example, we can see that there are lots of vulnerabilities between 9.0 – 9.5 but not many between 5.0 – 6.0]

Top Risks

1. **Unauthenticated X11 Server**
2. **DROWN Vulnerability**
3. **Vulnerable Oracle**

Remediation



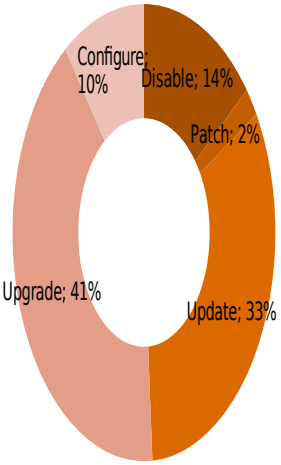
Staging.xl

[This Pie Chart helps visualize the breakdown of remedial actions by category. The objective is to put into perspective the effort (time and resources) required to close the vulnerabilities. For example, a vulnerability which requires structural reconfiguration in the way it is setup (i.e. workflow, permissions) will require significantly more effort to fix, than a vulnerability that simply requires a pre-existing patch already released by the vendor to be

Scan Type

77 %

Remediation



[Th
visu
vul
tha
and
env
The
per
app
critical to non-critical flaws, so remedial action can be budgeted for and prioritized accordingly]

Top Risks

1. **Outdated Red Hat Linux**
2. **Vulnerable .NET framework**
3. **Vulnerable MS**

*Detailed findings can be found in the hyperlinked .xls

of Vulnerabilities

CVSS

[This Scatter Graph helps visualize the breakdown of vulnerabilities by CVSS. The objective is to be able find clusters that indicate where most vulnerabilities lie. For example, we can see that there are lots of vulnerabilities between 8.0 – 9.0 but not many between 5.0 – 7.0]

[This Pie Chart helps visualize the breakdown of remedial actions by category. The objective is to put into perspective the effort (time and resources) required to close the vulnerabilities. For example, a vulnerability which requires structural reconfiguration in the way it is setup (i.e. workflow, permissions) will require significantly more effort to fix, than a vulnerability that simply requires a pre-existing patch, already released by the vendor, to be simply applied]

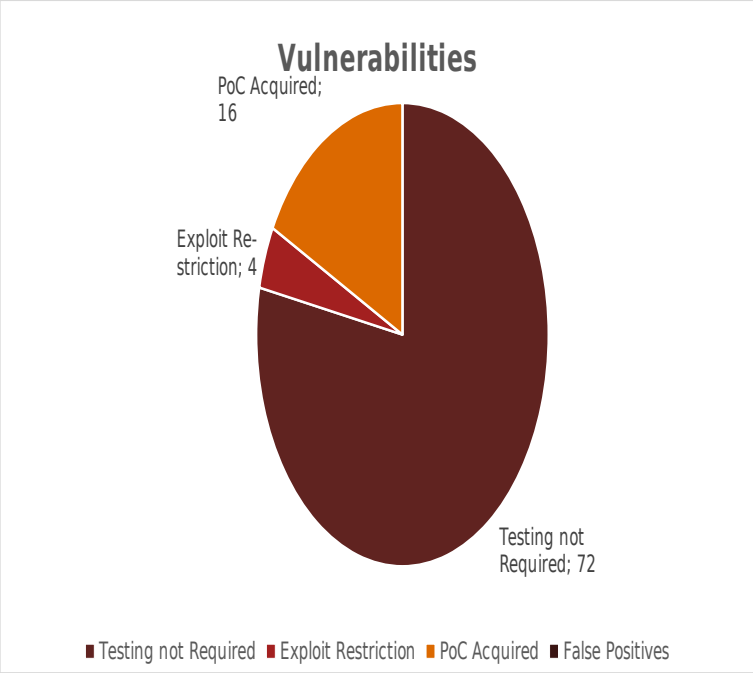
Disable: Removing a functionality, service or technology option
Patch: Applying a security patch publicly released by vendor
Update: Updating the version of a package or dependency
Upgrade: Upgrading underlying software or technology
Configure: Reconfiguring the setup and functionality


Mixed.xls

8. Internal Penetration Test Findings

38 IP Addresses Tested Extensively

(Only Staging IPs selected in order not to impact the Production Environment)



Testing not required: Outdated packages which don't require verification through exploitation

Exploit Restriction Require exploits that cause denial of service that would create operational issues

False Positives: Any findings mistakenly identified by automated scanning verified to be untrue

PoC Acquired: All findings that were exploited have corresponding screenshots embedded

67 STC Linux Production IPs **51 STC Windows Servers**

10.21.196.138	172.20.208.174	172.20.210.11	10.21.196.137	172.20.208.155	10.21.196.134
10.21.35.49	172.20.208.175	172.20.210.13	10.21.36.104	172.20.208.156	10.21.196.135
10.21.35.50	172.20.208.179	172.20.210.14	10.21.36.105	172.20.208.158	10.21.196.136
10.21.36.100	172.20.208.180	172.20.210.15	10.21.36.106	172.20.208.159	-
10.21.36.101	172.20.208.190	172.20.210.16	10.21.36.107	172.20.208.162	-
10.21.36.102	172.20.208.191	172.20.210.20	10.21.36.108	172.20.208.192	-
10.21.36.103	172.20.208.61	172.20.210.21	10.21.36.109	172.20.208.63	-
10.21.62.16	172.20.208.62	172.20.210.32	10.21.36.110	172.20.208.64	-
10.21.62.17	172.20.208.67	172.20.210.33	10.21.36.111	172.20.208.65	-
10.21.62.18	172.20.208.68	172.20.210.51	10.21.36.112	172.20.208.74	-
10.21.62.19	172.20.208.69	172.20.210.52	10.21.36.113	172.20.208.92	-
10.21.62.20	172.20.208.70	172.20.210.60	10.21.36.114	172.20.208.93	-
10.21.62.21	172.20.208.71	172.20.210.61	10.21.62.11	172.20.208.94	-
10.21.63.7	172.20.208.72	172.20.210.72	10.21.62.12	172.20.208.95	-
10.21.63.8	172.20.208.73	172.20.210.73	10.21.62.13	172.20.208.97	-
172.20.208.149	172.20.208.75	172.23.122.254	10.21.62.14	172.20.208.98	-
172.20.208.151	172.20.208.76	172.23.123.1	10.21.62.15	172.20.210.12	-
172.20.208.152	172.20.208.77	172.23.123.2	10.21.62.9	172.20.210.22	-
172.20.208.153	172.20.208.78	172.23.123.71	10.21.63.5	172.20.210.23	-
172.20.208.154	172.20.208.82	-	10.21.63.6	172.20.210.24	-
172.20.208.163	172.20.208.90	-	172.20.208.146	172.20.210.45	-
172.20.208.167	172.20.208.91	-	172.20.208.147	172.20.210.46	-
172.20.208.170	172.20.208.96	-	172.20.208.148	10.21.196.132	-
172.20.208.171	172.20.210.10	-	172.20.208.150	10.21.196.133	-

Raw Nessus Production Scan Results

32 STC Linux Staging IPs **6 STC Windows Staging IPs**

172.20.209.15	172.20.218.102	172.20.218.140	172.20.218.22	172.20.209.8
172.20.209.20	172.20.218.108	172.20.218.15	172.20.218.5	172.20.218.104
172.20.209.23	172.20.218.110	172.20.218.16	172.20.218.6	172.20.218.109
172.20.209.24	172.20.218.13	172.20.218.17	172.20.218.7	172.20.218.133
172.20.209.25	172.20.218.132	172.20.218.18	172.20.218.8	172.20.218.135
172.20.209.29	172.20.218.134	172.20.218.19	172.20.218.9	172.20.218.14
172.20.209.30	172.20.218.137	172.20.218.20	172.20.218.97	-
172.20.218.101	172.20.218.138	172.20.218.21	172.20.218.10	-

Critica Hig Medium Low Info

8.1 Vulnerable software installation

Score:

Observation

Outdated and vulnerable version of software packages are being used in critical servers in S******* which may lead to unauthorized access and sensitive information disclosure

Finding Description

During the assessment we observed that critical servers in S******* network are running an outdated and vulnerable version of Red hat Linux software packages.

We noticed that the following vulnerable software packages of Red Hat Linux are running on affected servers:

1) MySQL is running version 5.625 which is affected by remote code execution vulnerability (CVE-2015-4766, CVE-2015-4904) which may allow an attacker/malicious insider to disrupt availability of the system and bring it down.

Affected Targets

ESB (172.20.218.10)

OMS DB Testing (172.20.218.16)

SSO (172.20.218.17)

SSO (172.20.218.18)

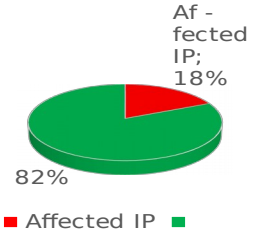
OMS TomCat Worker & DB (172.20.218.22)

SSO Testing (172.20.209.20)

OMS Testing (172.20.209.23)

MGM (172.20.218.140)

2) Apache httpd is running version 2.2.15 which is vulnerable to authentication bypass vulnerability (CVE-2017-3167) and may allow an attacker/malicious insider to bypass authentication requirement.



3) Kernel software package is running version 2.6.32-504.el6 which is affected by remote code execution vulnerability (CVE-2016-7117) which may allow an attacker/malicious insider to launch Denial of service attack.
4) Openssl is running version 1.0.1e-30.el6 which is by affected man-in-the-middle attack vulnerability (CVE-2015-3197) which may allow an attacker/malicious insider to downgrade the DHE connection to use export-grade key sizes and steal sensitive information.
5) Jasper-libs is running version 1.900.1-15.el6_1.1 which is affect by arbitrary code execution vulnerability (CVE-2014-8157) which may allow an attacker/ malicious insider launch denial of service attack.

Impact

An attacker or malicious insider may exploit vulnerability in these software packages to gain unauthorized access to the s******* critical system to execute arbitrary code and launch denial of service attack on the servers

Recommendation

We recommend to upgrade the software packages to the latest stable version

Screenshot

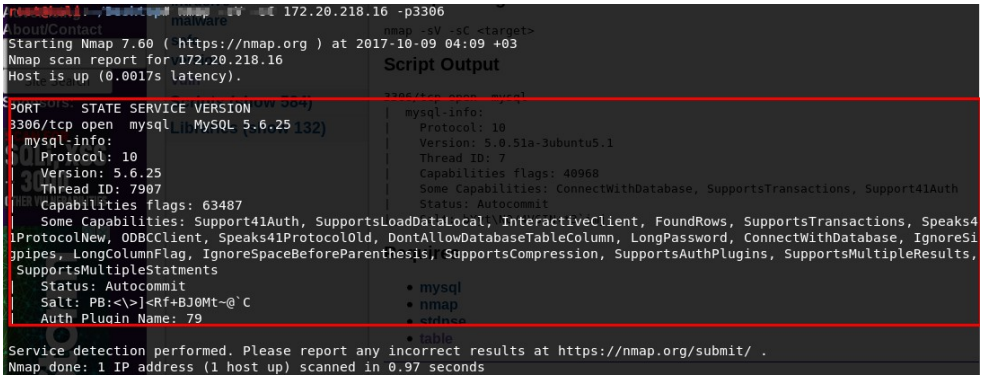


Figure 1

Figure 1: Shows the attacker can gain access to the facility admin screen from where the operating system can be

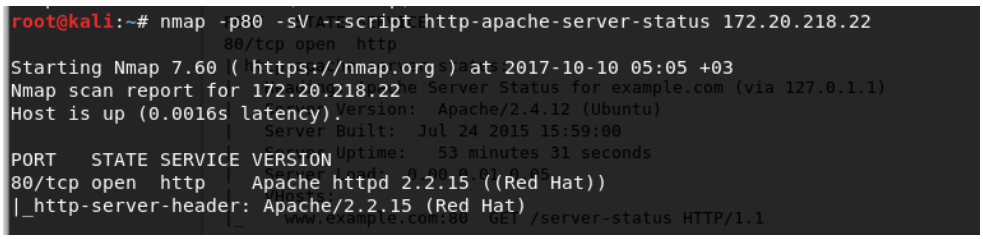


Figure 2

Figure 2: This particular version of Apache is vulnerable to authentication bypassing

8.2 Weak login credentials in Apache manager portal

Score: 9.8

Observation

Weak login credentials in Apache manager portal is used which may allow an attacker/malicious insider to gain unauthorized access to it, perform malicious activities and could bring the system down

Affected Targets

Avaya (172.20.218.104:8080)

Finding Description

During assessment we observed that default credentials (admin:****, tomcat:*****) are being used by Apache manager portal which may allow an attacker or malicious insider to gain unauthorized access.

Further, this may allow a malicious user to gain access to confidential information hosted on the system, modify and add malicious contents into the system.

Impact

An attacker or malicious insider may use this vulnerability to add new malicious content, modify or delete the existing system settings as well as could bring the system or service down.

Further, a malicious user may also upload malicious file on the server using admin rights to further gain unauthorized access to the network.

Recommendation

We recommend that easily guessable or default credentials should not be used should be replaced with a custom strong password, inline with password policy.

Screenshot

```
root@kali:~# nmap -p80 -sV --script http-apache-server-status 172.20.218.22

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-10 05:05 +03
Nmap scan report for 172.20.218.22
Host is up (0.0016s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.15 ((Red Hat))
|_http-server-header: Apache/2.2.15 (Red Hat)
```

Figure 1

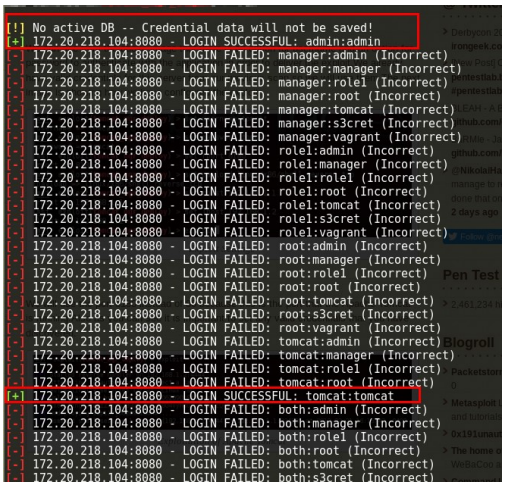


Figure 2

Figure 2: Default credentials are being used

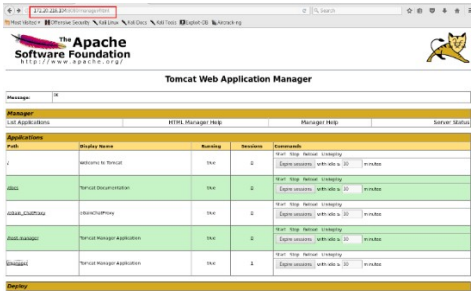


Figure 3: Exposed Web interface portal from using default login credential

8.3 ESB server found vulnerable to SMTP User enumeration

Score:

Observation

S******* ESB server found vulnerable to SMTP User enumeration which may allow an attacker to obtain a list of valid users and potentially gain unauthorized access to the system

Affected Targets

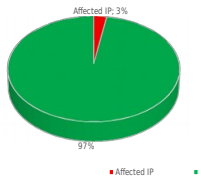
ESB (172.20.218.9:25)

Finding Description

We observed that it is possible to perform username enumeration using misconfigured SMTP service and gather information about mail server's users by sending malicious requests to the S******* ESB system.

During assessment we enumerated the following valid usernames without authentication:
Root
Administrator
Aphossam
Hpsim
qscan

Impact



An attacker or malicious insider may exploit this vulnerability to gain unauthorized access to the email server and perform malicious activities on the system to gain unauthorized access to the network.

Recommendation

We recommend that SMTP server should be reconfigured in a way that it does not reveal any sensitive information. Also, configure SMTP server to disallow the usage of the command VRFY.

Screenshot

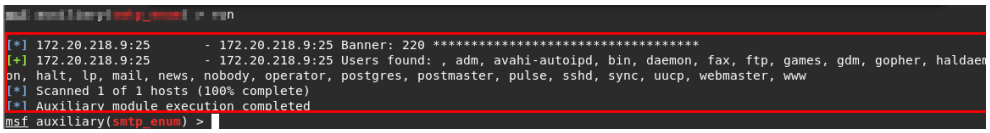


Figure 1

Figure 1: SMTP users can be listed out by an attacker and used to brute force credentials

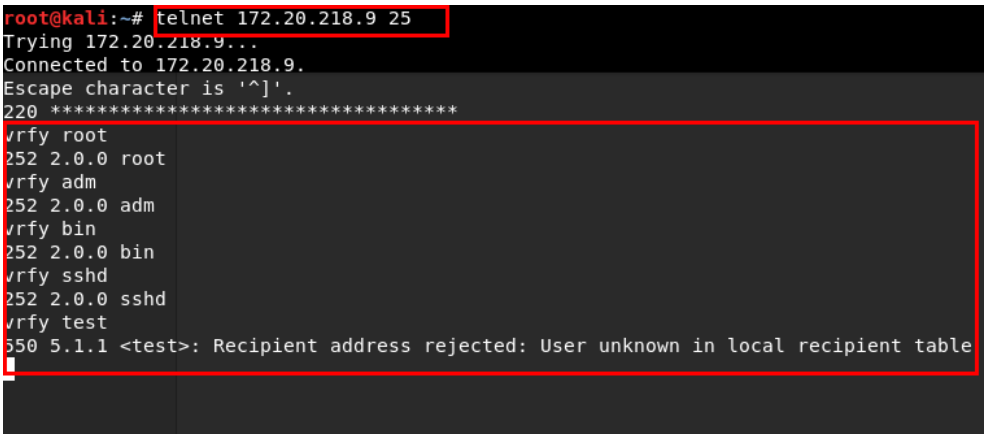


Figure 2

Figure 2: Shows that the VRFY account is enabled and can be used to check which users available on the local recipient table

8.4 Vulnerable X11 Service found running on critical Oracle OAM server

Score: 6.4

Observation

Vulnerable X11 Service found running on critical Oracle OAM server which may allow an attacker to steal potentially sensitive information

Affected Targets

Oracle OAM test server (172.20.218.109:6000)

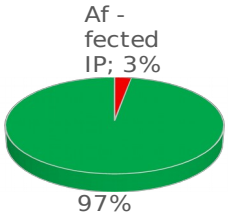
Finding Description

During assessment we observed that vulnerable x11 service is running on s******* system.
X11 service is a client-server protocol which is used to display graphical applications running on the system accepts connections from anywhere and any host.

This service may allow an attacker/malicious insider to gain unauthorized access to potentially sensitive information by connecting to the server to monitor the keystrokes and mouse event of the victim's system and gain unauthorized access to it.

Reference: CVE-1999-0526

Impact



An attacker/malicious insider may exploit this vulnerability to obtain the username and password of the victim's system by monitor keystrokes and mouse event.

Recommendation

We recommended to disable X11 client/server service if it is not being used or restrict access to this port by using the 'xhost' command.

Screenshot

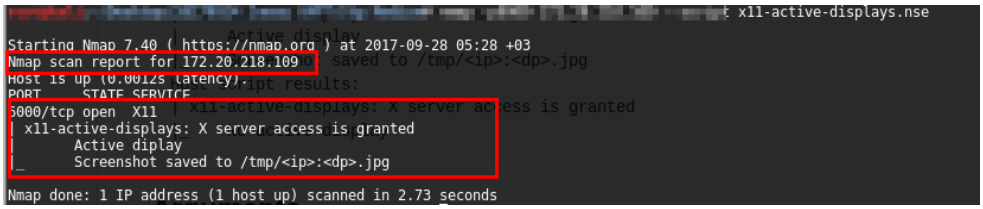


Figure 1

Figure 1: X11 indicates that an active display is detected to a remote user sniffing the network and then allows the user to

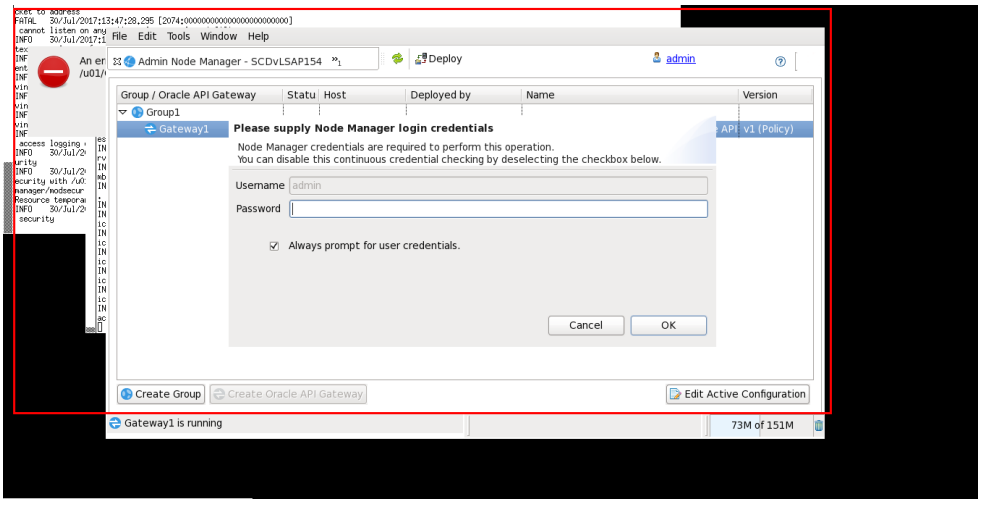


Figure 2

Figure 2: Screenshot that was captured

8.5 Insecure clear text protocol services FTP and HTTP found Score:

Observation

Insecure clear text protocol services FTP and HTTP found being used by the system which may allow an attacker/malicious insider to steal potentially sensitive information to gain unauthorized access to it

Affected Targets

Avaya (172.20.218.104:8080)

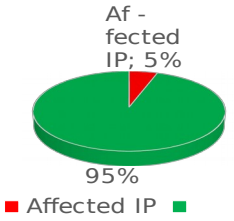
ODS (172.20.218.137:21)

Finding Description

During the assessment we observed that clear-text protocols FTP and HTTP are enabled on ODS and Avaya servers which may allow an attacker/malicious insider to steal sensitive information like login credentials to gain unauthorized access to the s******* system.

Impact

FTP and HTTPs is insecure services through which data is transmitted in clear-text.
A malicious user may see the sensitive information like user credentials and gain access to system. It may be used by a malicious attacker/insider to further gain access and gain further unauthorized access to the network.



Recommendation

We recommend to disable FTP services on the affected servers and use secured alternative as sftp for ftp and HTTPS instead of HTTP.

Screenshot

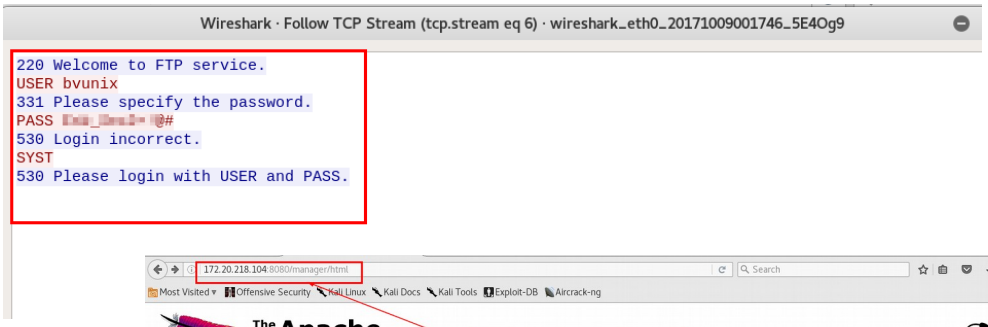


Figure 1

Figure 1: FTP can be seen running in unsecured clear text fashion

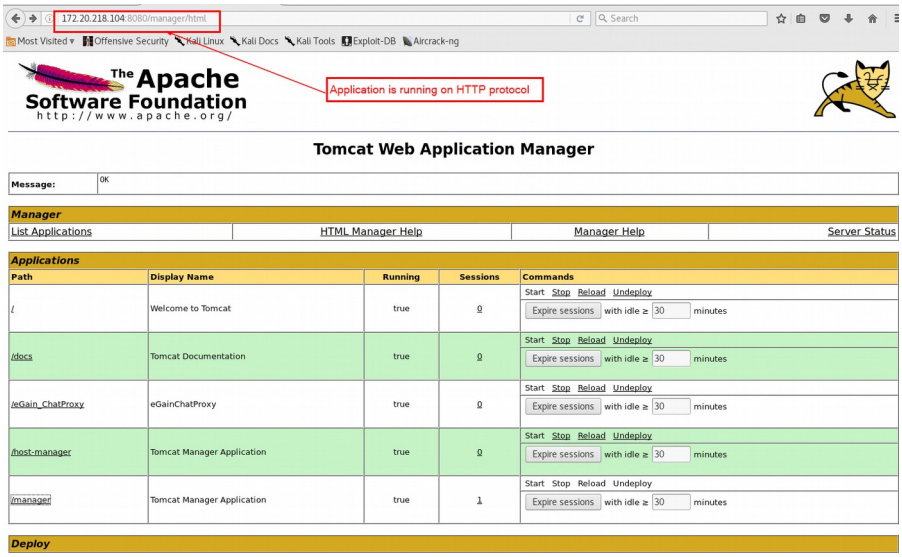


Figure 2

Figure 2: Application can be seen running over cleartext HTTP protocol

8.6 SMB signing found disabled

Score:

Observation

SMB signing, which is used for securing shared access to files, printers etc., found disabled which may allow an attacker to steal sensitive information and gain unauthorized access to S******* network.

Affected Targets

eGain
(172.20.218.14:445)

Avaya
(172.20.218.104:445)

(BI Tableau - STG)
172.20.218.133:445

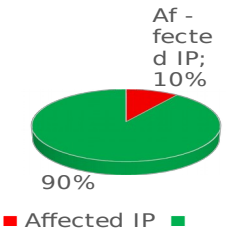
(BI Tableau - STG)
172.20.218.135:445

Finding Description

During assessment we observed that SMB signing is disabled on S******* eGain, BI Tableau - STG and BI Tableau - STG server. SMB is mainly used for providing shared access to files, printers.

SMB signing is a security mechanism in the SMB protocol which allows the recipient of SMB packets to confirm their authenticity and adds security to a network using NetBIOS, avoiding man-in-the-middle attacks. When SMB signing is enabled on both the client and server SMB sessions are authenticated between the machines on a packet by packet basis.

Impact

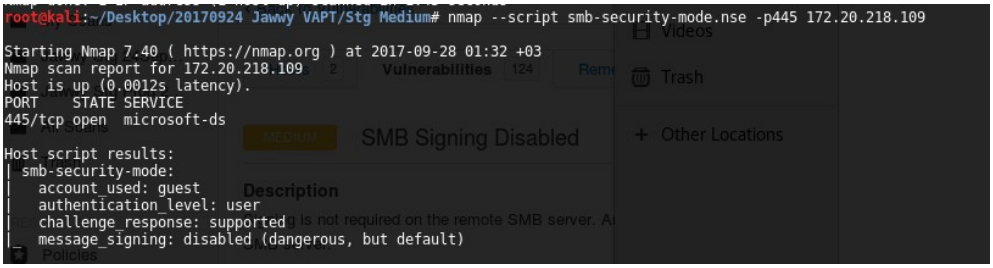


If SMB signing is disabled, it may allow unauthorized attacker/malicious insider to sniff the network and catch challenge/response exchanges and replay the whole process to grab session keys and authenticate on local network.

Recommendation

We recommend that SMB signing should be set to "enabled and required" on all affected servers.

Screenshot



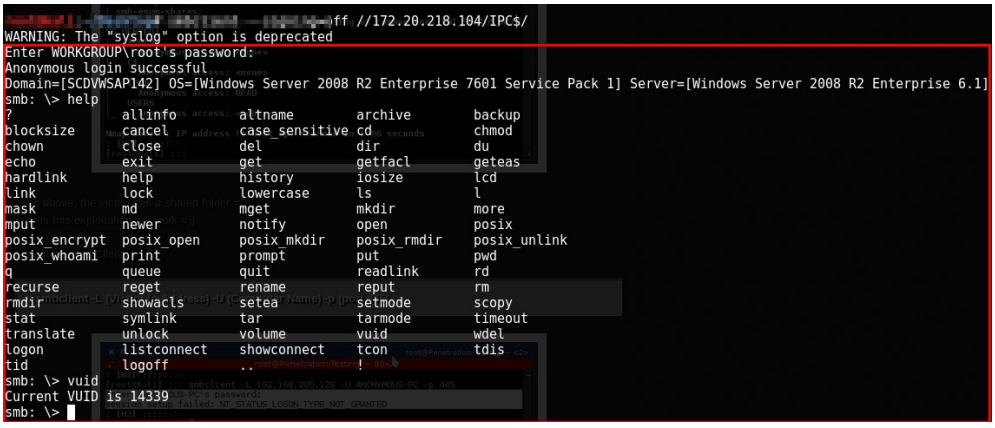


Figure 1

Figure 1: Server allows anonymous access to SMB services without

8.7 Server vulnerable to Oracle TNS listener poisoning attack

Score:

Observation

Oracle TNS listener poisoning attack which may allow an attacker to perform Man-in-the-Middle attack to steal potentially sensitive information

Affected Targets

ESB (172.20.209.25:1521)

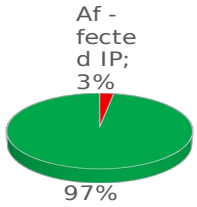
Finding Description

During the assessment, we observed that the Oracle database server is vulnerable to remote "TNS Listener Poison Attack".

An unauthorized attacker/malicious insider can register a malicious service with the database listener with the same service name as legitimate database service without authentication to perform Man-in-the-Middle attack. This will hep the attacker to gain unauthorized access to potentially sensitive information and redirect user data to malicious sites.

Reference: CVE-2012-1675.

Impact



If a malicious attacker/insider who is able to register to the oracle listener service, will divert all the traffic to the his/her machine causing a Man-in-The-Middle attack and all the requests or responses, sensitive information (usernames, passwords, personal information) will be passed through the attacker's machine which can be used by attacker to dig further in the network, and gain access to sensitive information.

Recommendation

We recommended the configuration change "DYNAMIC_REGISTRATION_LISTENER=OFF " in listener.ora file .

Screenshot

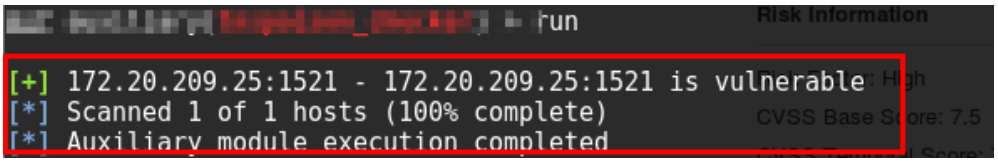


Figure 1

Figure 1: TNS Listener is vulnerable to the attacker performing a man in

8.8 Network Level authentication (NLA) is not being used for RDP connections

Score:

Observation

Network Level authentication (NLA) is not being used for RDP connections on system which may allow an attacker/malicious insider to perform Man-in-the-Middle attack to steal potentially sensitive information

Affected Targets

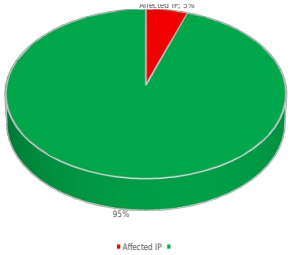
Avaya (172.20.218.104:3389)

Oracle OAM test server (old datamart) (172.20.218.109:3389)

Finding Description

During assessment we observed that Network level authentication is not being used for RDP connections on Avaya and Oracle OAM test servers.
Network Level Authentication completes user's authentication before a remote desktop connection is established and the logon screen appears. This is a more secure authentication method that can help and protect the remote computer from malicious users and/or software.

Impact



If an attacker/malicious insider gains access to the same network segment as the targeted system during an active Remote Desktop Protocol (RDP) session, he may temper the sensitive data and send crafted RDP packets to the targeted system and may launch denial of service attack on the targeted system.

Recommendation

We recommend that all affected server should be configured to require NLA for RDP connections.

Screenshot

```
[+] Scanning 1 hosts

Target:    172.20.218.109
IP:        172.20.218.109
Port:      3389

[+] Checking supported protocols

[-] Checking if RDP Security (PROTOCOL_RDP) is supported...Supported
[-] Checking if TLS Security (PROTOCOL_SSL) is supported...Supported
[-] Checking if CredSSP Security (PROTOCOL_HYBRID) is supported [uses NLA]...Supported

[+] Checking RDP Security Layer

[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_NONE...Not supported
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_40BIT...Supported.  Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_128BIT...Supported.  Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_56BIT...Supported.  Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_FIPS...Supported.  Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

[+] Summary of protocol support

[-] 172.20.218.109:3389 supports PROTOCOL_RDP   : TRUE
[-] 172.20.218.109:3389 supports PROTOCOL_HYBRID: TRUE
[-] 172.20.218.109:3389 supports PROTOCOL_SSL   : TRUE

[+] Summary of RDP encryption support

[-] 172.20.218.109:3389 has encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] 172.20.218.109:3389 supports ENCRYPTION_METHOD_NONE   : FALSE
[-] 172.20.218.109:3389 supports ENCRYPTION_METHOD_40BIT  : TRUE
[-] 172.20.218.109:3389 supports ENCRYPTION_METHOD_128BIT : TRUE
[-] 172.20.218.109:3389 supports ENCRYPTION_METHOD_56BIT  : TRUE
[-] 172.20.218.109:3389 supports ENCRYPTION_METHOD_FIPS   : TRUE

[+] Summary of security issues

[-] 172.20.218.109:3389 has issue WEAK_RDP_ENCRYPTION_SUPPORTED
[-] 172.20.218.109:3389 has issue SSL_SUPPORTED_BUT_NOT_MANDATED_MITM
[-] 172.20.218.109:3389 has issue FIPS_SUPPORTED_BUT_NOT_MANDATED
[-] 172.20.218.109:3389 has issue NLA_SUPPORTED_BUT_NOT_MANDATED_DOS

rdp-sec-check v0.9-beta completed at Mon Oct  9 01:36:14 2017
```

Figure 1

Figure 1: Lack of mandated NLA allows attacker to setup RDP connection without authentication

8.9 Vulnerable HTTP method (TRACE) is enabled

Score:

Observation

Vulnerable HTTP method (TRACE) is enabled on the system which may allow an attacker to steal sensitive information like user's login session to gain unauthorized access to legitimate user account

Affected Targets

ESB
(172.20.218.10:443)

ESB/Git/Nexus
(172.20.218.6:9088)

BI - ETL Dev/STG
(172.20.218.132:80)

ODS
(172.20.218.137:80)

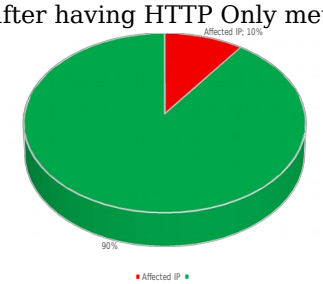
Finding Description

During the assessment, we observed that vulnerable HTTP method TRACE is enabled on ESB, ESB/Git/Nexus system, which may allow an attacker/malicious insider to steal legitimate user's session to gain unauthorized access to legitimate user accounts.

Reference: CVE-2010-0386

Impact

TRACE method echoes back what is sent in the request. Here, if the browser has a cookie for the domain, then, that cookie will also be reflected in the response and then can be accessed by JavaScript to be used further attacks, after having HTTP Only method enabled.



When the attacker gets hold of the cookies of a legitimate user, then he/she can perform operations in the application hosted on the server or on the server directly as the legitimate user which may directly impact the Organization's data.

Recommendation

We recommend that TRACE method should be disabled on all affected servers.

Screenshot

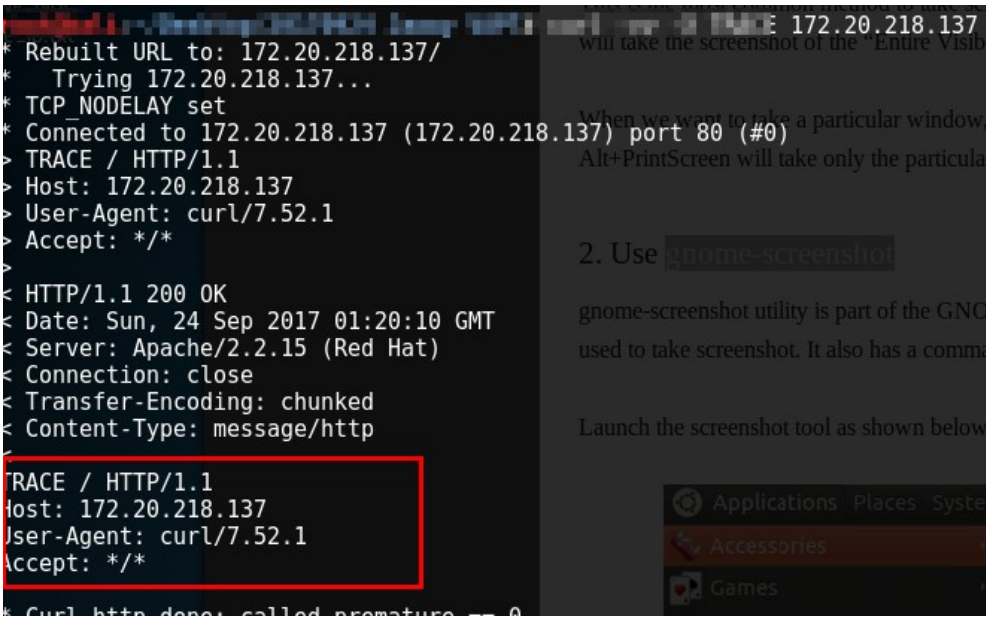


Figure 1

Figure 1: Trace HTTP method is allowed and can potentially allow attacker to steal a user session

Score:

8.10 Servers found vulnerable to POODLE attack

Observation

S******* servers found vulnerable to POODLE attack whose SSL versions having multiple vulnerabilities are being used to transmit sensitive information in the S******* network which may allow an attacker to gain unauthorized access to sensitive data like passwords may allow an attacker to gain unauthorized access to sensitive data like passwords

Affected Targets

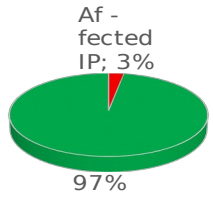
ESB (172.20.218.10:443)

Finding Description

During the assessment, we observed that critical server in S******* network is affected by POODLE vulnerability which allows an attacker to carry out Man-In-The-Middle attack by forcing an application to repeatedly send the same data over SSL 3.0 connections and decrypt encrypted messages thereby gaining unauthorized access to sensitive information. As long as the client and server support SSLv3, a connection can be rolled back to SSLv3 thus enabling this vulnerability.

Reference: CVE-2014-3566

Impact



By exploiting this vulnerability an attacker can gain access to sensitive data passed within the encrypted sessions, such as passwords that can then be used to gain further access on systems.

Recommendation

We recommend that SSLv3 should be disabled on all affected systems and TLS should be used instead on all affected systems. Additionally, services that require SSLv3 should enable the TLS fallback SCSV mechanism until SSLv3 can be disabled.

Screenshot

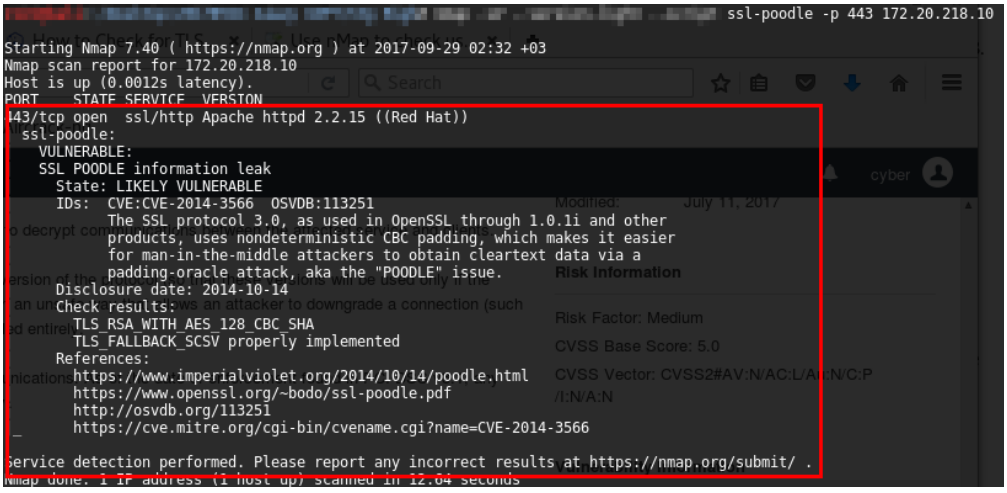


Figure 1

Figure 1: Indicates that server allows SSL connection to be downgraded if chosen

8.11 Weak SSH Algorithm is supported by the critical system

Score:

Observation

S******* ESB server found vulnerable to SMTP User enumeration which may allow an attacker to obtain a list of valid users and potentially gain unauthorized access to the system

Finding Description

During assessment we observed that SSH server is configured to use the Arcfour stream cipher and MD5, SHA1 or no cipher to the targeted critical OMS App Testing, OMS DB Testing, SSO Testing, SAP HANA, ODS system, which may allow an attacker to steal users sensitive information like user's session and gain unauthorized access to system.

Impact

Arcfour is not to be used as it has weak keys. The Arcfour cipher is compatible with the RC4 cipher with weak key. An attacker/malicious insider who have access to network data can exploit this vulnerability to display plaintext from a block of ciphertext and obtain sensitive information.

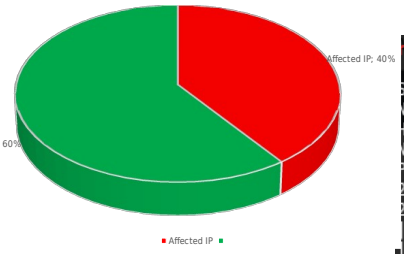
Recommendation

We recommend that weak ciphers such as arcfour should be disabled on all affected systems.

Affected Targets

OMS App Testing (172.20.209.15)
SSO Testing (172.20.209.20)
MGM (172.20.218.140)
OMS Testing (172.20.209.23)
SSO (172.20.218.17)
OMS DB Testing (172.20.218.16)
OMS App Testing (172.20.218.15)
OMS (172.20.218.21)
SSO (172.20.218.18)
ESB (172.20.218.9)
ESB (172.20.218.8)
ESB (172.20.218.7)
ESB (172.20.218.10)
OMS TomCat Worker & DB (172.20.218.22)
ESB (172.20.209.24)
RMS (172.20.218.97)
ESB (172.20.209.25)
ESB/Git/Nexus (172.20.218.6)
Oracle OAM (old datamart) (172.20.218.108)
Oracle OAM (old datamart) (172.20.218.110)
ESB/JON (172.20.218.5)
[illegible]

Screenshot




```
root@kali:~/Desktop/20170924 Jawwy VAPT/Stg High# nmap -Pn --script ssh2-enum-algos 172.20.209.15

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-29 01:58 +03
Nmap scan report for 172.20.209.15
Host is up (0.0053s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (6)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
|       arcfour128
|       arcfour
|   mac_algorithms: (9)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|       zlib@openssh.com
23/tcp   closed telnet
113/tcp  closed ident
1521/tcp closed oracle
3306/tcp open   mysql
```

Plugin Details

Severity:	Medium
ID:	90317
Version:	$Revision: 1.3 $
Type:	remote
Family:	Misc.
Published:	April 4, 2016
Modified:	December 14, 2016

Risk Information

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/I:N/A:N

Figure 1: Weak SSH ciphers are vulnerable to be being cracked by an attacker so he can

Figure 1

8.12 Disclosure of sensitive information

Score:

Observation

Multiple servers in S******* network found misconfigured to display default page which may lead an attacker/malicious insider to disclosed sensitive information about the backend technology

Affected Targets

RMS (172.20.218.97:8080)

ODS (172.20.218.137:8080)

BI - ETL Dev/STG (172.20.218.132)

Finding Description

During assessment, we observed that, the targeted system is misconfigured to display default apache and Servlets pages, which may disclosed sensitive information about the backend technology. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

Impact

This default configuration reduces the attack surface of target application/server as a malicious user may launch known attacks.

Recommendation

We recommend to disable the service if it is not being used or hide or delete default pages.

Screenshot

Figure

Figure 1: Default Apache page reveals web stack and software details

8.13 Weak encryption method RC4 used

Score:

Observation

Weak encryption method RC4 found being used in remote desktop connections which may allow an attacker to steal potentially sensitive information

Affected Targets

Oracle OAM test server (old datamart) (172.20.218.109:3389)

Avaya (172.20.218.104:3389)

BI Tableau - STG (172.20.218.133:3389)

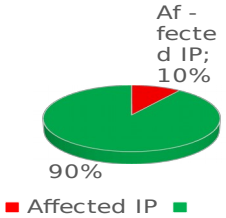
BI Tableau - STG (172.20.218.135:3389)

Finding Description

During assessment we observed that weak cipher like RC4 is being used when RDP sessions is created on the system, which may allow an attacker/ malicious insider to steal sensitive information. RDP is not considered secure due to multiple flaws present in it and does not prevent the connection from MiTM attacks.

Reference: CVE-2005-1794

Impact



This flaw may allow an attacker to potentially perform a man-in-the-middle attack where a user has just negotiated an encrypted connection with some malicious third-party who is decrypting everything and then re-encrypting it to send to the real server. This can happen on initial contact.

Recommendation

We recommend that stronger cipher suites should be used for RDP connections.

Screenshot

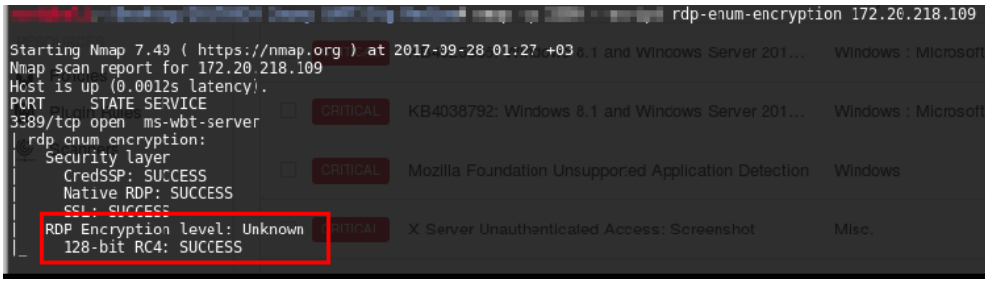


Figure 1

Figure 1: 128-bit RC4 cipher prone to being cracked is available for use for desktop connections

8.14 Weak cipher having multiple vulnerabilities used

Score:

Observation

Weak cipher having multiple vulnerabilities are being used to transmit sensitive information in the network which may allow an attacker/malicious insider to steal potentially sensitive information

Affected Targets

RMS
(172.20.218.97:9443)

ESB
(172.20.218.10:443)

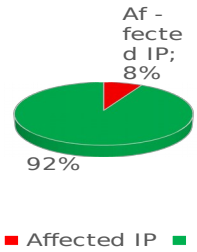
ESB/JON
(172.20.218.5:383)

Finding Description

During assessment we observed that weak cipher like RC4-SHA, RC4-MD5 DES-CBC3-SHA, 64-bit block cipher 3DES and protocol TLsv1.0 having multiple vulnerabilities are being used to transmit sensitive information in the network which may allow an attacker/malicious insider to steal sensitive information.

Reference: CVE-2016-6329

Impact



RC4 stream ciphers, CBC-mode block ciphers, 64-bit block cipher 3DES is known to be vulnerable to information leakage vulnerability, which allows an attacker/malicious insider to decrypt the communication between the client & server, which may lead to stealing of the sensitive information such as "Secure HTTP Cookies" flowing between the client and server.

Recommendation

We recommended that vulnerable SSL services, i.e. SSLv3 and TLS1.0, should be disabled and use TLS V1.1 or later for encrypting the data in transit.
We recommended to disable support for export cipher suites and use 2048-bit Diffie-Hellman group.
Upgrade the system to TLS1.2 and utilize AES-GCM (for RC4)

Screenshot

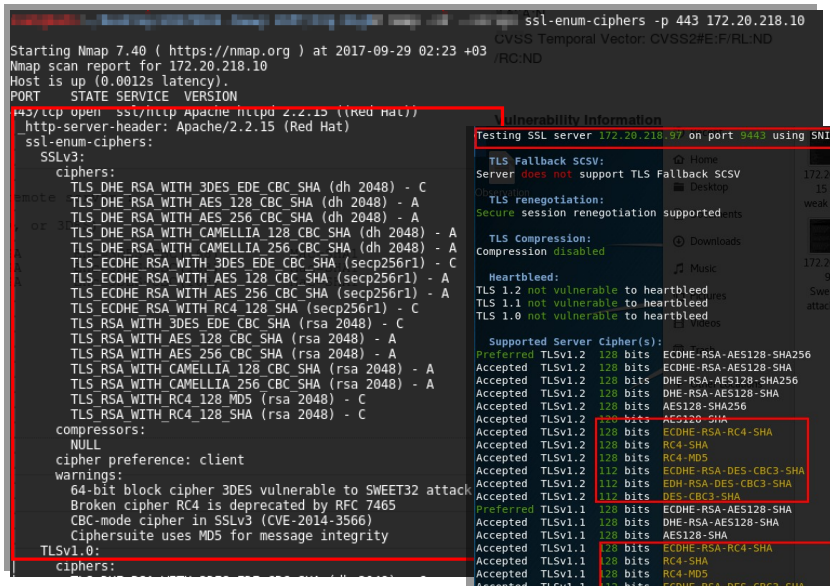


Figure 1

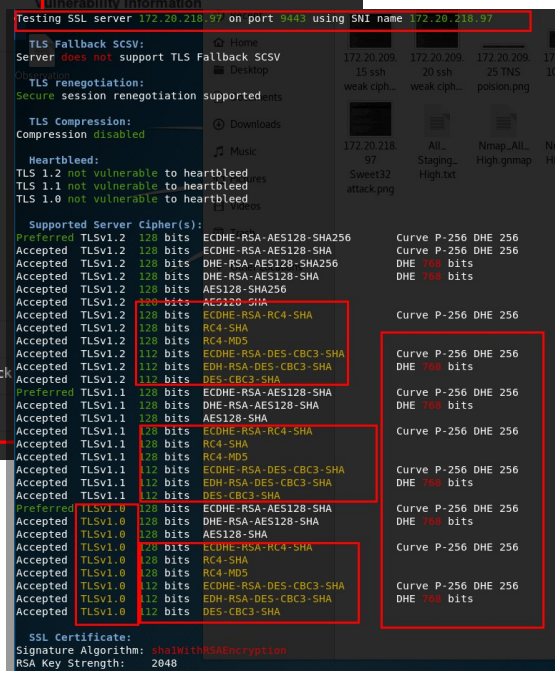


Figure 2

Figure 1: Broken cipher that uses limited 64-bit block sizes is used which can lead to attacker stealing session cookies by producing

Figure 2: Host of extremely weak ciphers for SSL services including 64-bit 3DES available to be used for client server

8.15 Server vulnerable to Slowloris Denial-of-service attack

Score:

Observation

Multiple servers in S******* network found vulnerable to Slowloris Denial-of-service attack which may allow an attacker/malicious insider to launch Denial of service attack on the systems and render the service running on it unavailable.

Affected Targets

RMS (172.20.218.97:8080)

SSO (172.20.218.17:80)

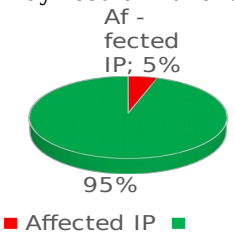
Finding Description

We observed that the multiple servers in S******* network is affected by a denial of service vulnerability due to improper validation of queries. Slowloris tries to keep an http session active continuously for long period of time.

Slowloris is not noticed by IDS (Intrusion Detection system's), because it does not send a malformed request, but a legitimate request to the web server.

Impact

An unauthenticated attacker/malicious insider can exploit this vulnerability which may result in unavailability of system/device to legitimate users.



Recommendation

We recommend that applications should be reconfigured to mitigate this type of Denial of service attacks by reconfiguring mod_reqtimeout to set timeouts for receiving the HTTP request headers and the HTTP request body from a client.

Screenshot

```
slowloris-check 172.20.218.17 -p80

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-09 03:57 +03
Nmap scan report for 172.20.218.17
Host is up (0.0017s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/

Nmap done: 1 IP address (1 host up) scanned in 311.54 seconds
```

Figure 1

Figure 1: Verifies that web server is prone to exhaustion if partial requests are intentionally sent to keep connections active to cause denial

8.16 Vulnerable SMB service enabled

Score:

Observation

SMB service, which is used for providing shared access to files, printers etc., found vulnerable to information disclosure vulnerability which may reveal sensitive information to attacker/malicious insider

Affected Targets

Avaya
(172.20.218.104:445)

Oracle OAM test server (old datamart)
(172.20.218.109:445)

BI Tableau - STG
(172.20.218.135:445)

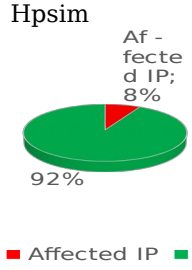
Finding Description

During the assessment we observed that SMB is configured in a way that which may disclose sensitive information which may allow an attacker/malicious insider to gain unauthorized access to the system and steal sensitive information.

SMB is used for providing shared access to files, printers and miscellaneous communications between nodes on a network.

During assessment we found following valid usernames:

- Administrator
- Aphossam
- Hpsim



- Qscan
- Visitor

Reference: CVE-1999-0520

Impact

This vulnerability may allow an attacker/malicious insider to gain unauthorized access to the system and steal potentially sensitive information.

Recommendation

We recommend to set access restrictions on shares for all affected servers. Remove all unnecessary users that exist on the server for e.g. 'hpsim'

Screenshot

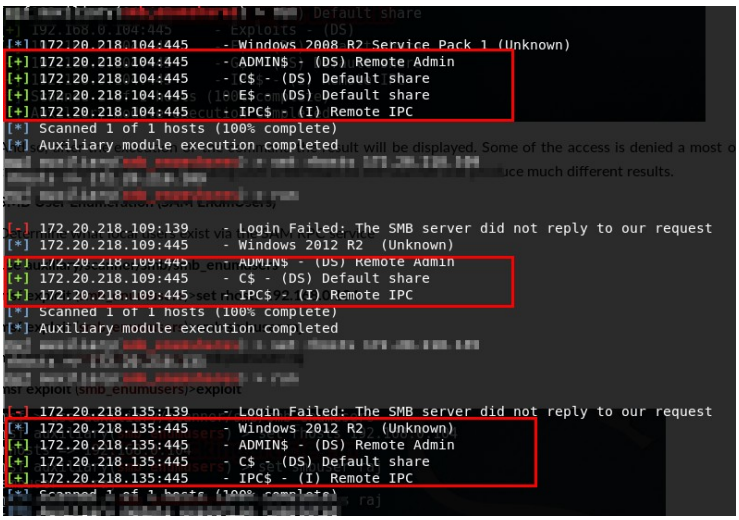


Figure 1

Figure 1: SMB Shares are visible and can be

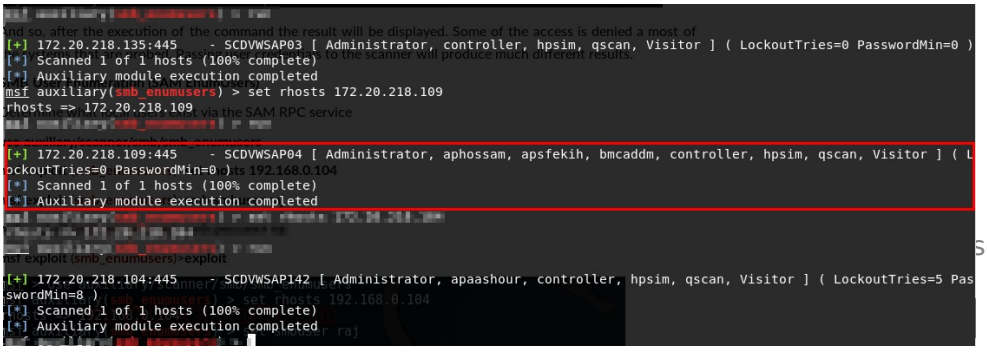


Figure 2

Figure 2: SMB User Accounts enumerated and visible

Appendices

Appendix – Common Vulnerabilities & Exposures

What is CVE?

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of CVE is to make it easier to share data across separate vulnerability capabilities, tools, repositories, and services with a common enumeration

Who owns CVE?

CVE is sponsored by US-CERT and copyrighted by MITRE for the benefit of the community to ensure it remains a free and open standard, as well as to legally protect the ongoing use of it and any resulting content by government, vendors or users.

How can CVE help?

CVE helps because it provides a standardized identifier for a given vulnerability or exposure to allow quick and accurate determination of which tools are most effective and appropriate for the organization's needs.

Is there a lot of support for something like this?

CVE is industry endorsed by the CVE Numbering Authorities (CNAs), CVE Board, and numerous organizations that have declared their products CVE-Compatible and include CVE Identifiers in their vendor alerts and security advisories

Is CVE just another vulnerability database?

CVE is not a vulnerability database but instead designed to allow vulnerability databases and other capabilities to be linked together to facilitate comparison of security tools and services

What is a vulnerability?

A vulnerability is a weakness in the computational logic found in software and some hardware components that, when exploited, results in a negative impact to confidentiality, integrity or availability

What is an exposure?

An exposure is a system configuration issue in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network