REPORT

ACME Test Industries
Internal Vulnerability Assessment Report

Oct 1st, 2099

ACCELERATING DIGITAL TRANSFORMATION

U.S. HEADQUARTERS
3 SEAVIEW BOULEVARD
PORT WASHINGTON, NY
11050

AGILANT
SOLUTIONS INC

1 DOCUMENT CONTROL

APPROVAL

The signatures below certify that this document has been reviewed and accepted and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

	Name	Position
Prepared by	Steven Forti	Chief Information Security Officer
Prepared by	Vincent Gulino	Senior Security Architect
Reviewed by	Harry Taluja	Chief Technology Officer
Reviewed by	Katie Riley	Director, Business Development & Marketing

AMENDMENT RECORD

This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

Page No.	Context	Revision	Date

COMPANY PROPRIETARY INFORMATION

The electronic version of this document is the latest revision. It is the responsibility of the individual to ensure that any paper material is the current revision. The printed version of this manual is uncontrolled, except when provided with a document reference number and revision in the field below:

Document Ref. _____ Rev _____

Uncontrolled Copy [•] Controlled Copy [ ] Date _____

2 EXECUTIVE SUMMARY

ACME Test Industries (herein "ACME") engaged Agilant Solutions, Inc. (herein "Agilant") to conduct a comprehensive vulnerability assessment which consisted of testing a multitude of systems which reside both internally & externally.

The Internal phase of the assessment was conducted (inside assessment) and this report describes the results, the methodology employed, the overall risk to the organization and the effectiveness of the components tested. It also provides recommendations for mitigating risk through configuration changes and/or technology investments, where appropriate.

Based on the results of the vulnerability assessment, Agilant is providing a summary of the overall observations and will include detailed recommendations on next steps later in the document.

Speaking specifically to the inside core network of the ACME Test Industries which is partitioned from the untrusted internet by a series of security investments including a perimeter firewall and an inline IPS solution the overall consensus is that the security posture requires improvement. This is not to say the infrastructure is left without protection as the implementation of the Carbon Black endpoint solution which was spearheaded by the local IT department was a very prudent & worthwhile investment.

However, with respect to the likelihood of breach, the landscape changes drastically and very quickly and since there are other areas where both investments and additional changes can be made to further strengthen the barrier it would be wise to do so as soon as possible.

Overall, similar to the findings noted during the outside vulnerability assessment many systems were found to be aging, unsupported, sub optimally configured and incapable of combating more modern threats due to outdated versions of software. Additionally, the placement and volume of data produced by these systems in their entirety more than likely have the effect of overwhelming it staff with superfluous, and in some instances difficult to interpret datasets, which can cause valuable information which must be acted upon expeditiously to become lost and/or buried.

It is for the aforementioned reasons one of Agilant's primary recommendations resulting from this test is to collapse the services of several perimeter devices into a single HA pair of NGFW devices which can accomplish the tasks of each device slated for retirement with far greater efficiency, ease of use and simplicity in design.

3 USING THIS REPORT

This report contains several sections that are helpful to different groups of people.

- The **Scope** section describes the boundaries of the Vulnerability assessment.
- The **Findings and Recommendations** section contains detailed information on the vulnerabilities identified during the Vulnerability assessment. The findings are structured in a table format so they can be placed into other reports. This allows ACME Test Industries to give area owners only the findings that pertain to their security responsibilities.
- The **Risk Assessment** section evaluates the probability of the worst case scenarios
- The **Recommendation prioritization** section provides guidance on what our consultants feel should be addressed first based on ease of implementation & overall effectiveness of change

4 SCOPE

ACME Test Industries engaged Agilant to conduct a comprehensive vulnerability assessment consisting of several components. To provide the best possible service to ACME Agilant has decided to break the overall report down into several sections "chunks" to make the information easier to assimilate and act upon expeditiously.

The tasks conducted were as follows:

- Conduct Kickoff Meeting: Agilant conducted a kickoff meeting with ACME Test Industries to review the objectives of the internal vulnerability assessment, to obtain any additional required information, and to exchange contact information.
- Perform a blind Inside Vulnerability Assessment: Agilant consultants enumerated and reviewed all of the internally accessible hosts through a services icmp echo replies and tcp services. A full network profile was constructed and compared to IP hosts provided by the customer and used to further isolate our efforts on hosts which exhibited a strong possibility of potential compromise
- Determine the overall impact on customer assets.
- Prepare this Report which represents the first in a series: Agilant prepared this document that details the findings and recommendations for the vulnerability assessment.
- Review final report with the customer to determine an appropriate action plan.

5 LEVELS OF RISK

Agilant risk ratings are defined as follows.

Critical -- The exposure is the most damaging of the high risk vulnerabilities. These weaknesses are typically exploited by self-propagating worms and have a myriad of publicly available exploit code on the Internet.

High -- The exposure may be exploited to produce adverse outcomes such as unauthorized privilege escalation, denial of service, data access, more than one percent downtime per month, or compromise of data. A high risk rating is given to vulnerabilities where ease of exploitation and impact of exploitation are both high.

Medium -- The exposure, when combined with other exposures, may be exploited to produce adverse outcomes such as downtime, system compromise, unauthorized privilege escalation, or unauthorized data access. A medium risk may also indicate a condition that does not expose the system to immediate risk, but may expose the system to risk in the future or is a deviation from best practices which could ultimately lead to negative outcomes from a regulatory and/or insurance based perspective.

Low -- The exposure does not contribute to a near-term adverse outcome, but provides further information about the system, application, or network.

Attention -- A finding rated as Attention does not have a risk high enough to be called a Low Risk finding. Rather, it is a finding that should be considered to improve security from an already acceptable level. Agilant believes appropriate risk mitigation and security controls exist within the system tested, but security could be further improved with the recommendations provided.

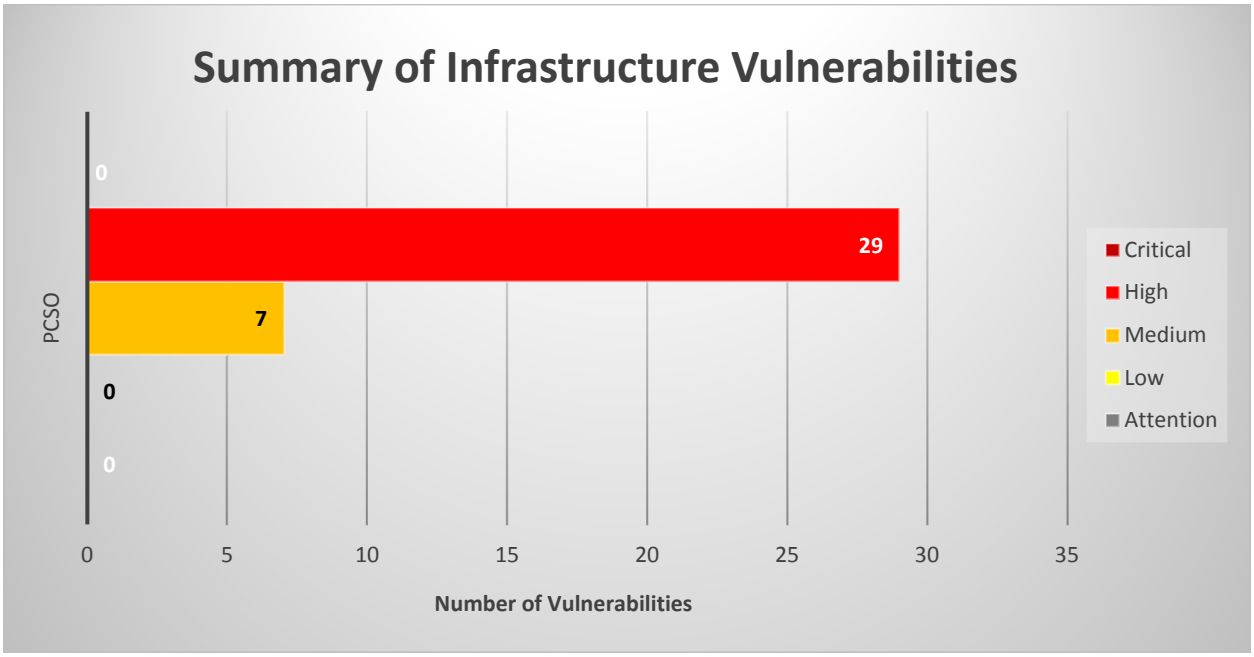
6 CONSOLIDATED SUMMARY OF FINDINGS

While performing the internal penetration test, the Agilant consultants revealed several areas of concern and several vulnerabilities that customer should address. The most critical findings fall within the following categories:

- Configuration parameters
- Device/software version
- Allowed & disallowed services
- Device/software support & age
- Patch Management

6.1 Summary of Infrastructure Vulnerabilities

This chart illustrates the number of vulnerabilities found during the internal penetration test. Details on the specific vulnerabilities are included in the "Findings and Recommendations" section below.



7 METHODOLOGY

7.1 Vulnerability Testing

Agilant Security Solutions conducted network-based vulnerability testing of the infrastructure and blind, unauthenticated testing of web applications. The objective of the penetration testing was to identify security weaknesses that could be exploited by motivated, malicious individuals to gain unauthorized access to the infrastructure. Where a flaw was identified, Agilant sought to verify the presence of said vulnerability through repeated scans using a variety of tools capable of testing for the same type of vulnerability. Agilant Security Solutions used a series of vulnerability scanning tools and manual techniques to identify, validate, and exploit security vulnerabilities. Testing was conducted in three phases: Discovery, Vulnerability Identification and Verification.

Phase I: Discovery
Agilant Security Solutions performed reconnaissance to gather information including registration data, operating system version and patch level, and service version and configuration.

Phase II: Vulnerability Identification
Agilant Security Solutions used a combination of commercial and open-source tools to identify security vulnerabilities in tested systems.

Phase III: Verification
Vulnerabilities identified by these tools were confirmed by our security staff to ensure there were no false positives.

7.1.1 Network & Web Vulnerability Tests

Agilant Security Solutions performed base level security scans of all the hosts to identify services and issues within these services. Once this was complete, manual techniques were employed to identify risks that automated tools cannot identify. The testing techniques included:

- DNS Queries: Query Name databases such ARIN to obtain domain names, IP address block assignments, and registrar information.
- Host Identification: Identify live hosts through ICMP, Reverse DNS, and port scans for common services.
- Network Route Mapping: Map the network route to each system using trace route and Visual Route.
- Operating System Identification: Identify the operating system of each host through analysis of responses to specially crafted TCP/IP packets.
- Network Services Enumeration: Enumerate the services available on each system through TCP and UDP port scanning by using tools such as NMAP.
- Network Service Exploration: Build a detailed profile of each service through automated and manual banner grabbing and service exploration without exploiting any service vulnerabilities.
- Vulnerability Identification: Use commercial and open-source vulnerability scanners to identify known vulnerabilities on each system.
- Vulnerability Exploitation: Use commercial, open source, and private exploitation tools and methods to gain access to the system or sensitive data.
- Agilant Security Solutions performed unauthenticated functional security testing of identified applications and attempted to gain unauthorized access to the application, hosting system, and sensitive data. The testing techniques included:

- Input validation bypass: Client-side validation routines and bounds-checking restrictions were removed to ensure controls are implemented on all application parameters sent to the server.
- SQL injection: Specially crafted SQL commands were submitted through input fields to validate whether input controls were in place to properly protect database data.
- Cross-site scripting: Active content was submitted to the application to cause a user's web browser to execute unauthorized and unfiltered code. This test was meant to validate user input controls.
- Parameter tampering: Query strings, POST parameters, and hidden fields were modified to gain unauthorized access to user data or application functionality.
- Cookie poisoning: Data sent in cookies was modified in order to test application response to receiving unexpected cookie values.
- Session hijacking: Agilant Security Solutions attempted to hijack a session established by another user to assume the privileges of that user.
- User privilege escalation: Agilant Security Solutions attempted to gain unauthorized access to administrator or other users' privileges.
- Credential manipulation: Agilant Security Solutions modified identification and authorization credentials to gain unauthorized access to other users' data and application functionality.
- Forceful browsing: Agilant Security Solutions enumerated files located on a web server to access files and user data not explicitly shown to the user within the application interface.
- Backdoors and debug options: Many applications may contain code left by developers for debugging purposes. Debugging code typically runs with a higher level of access, making it a target for potential exploitation. Application developers may leave backdoors in their code. Agilant Security Solutions identified these options that could potentially allow an intruder to gain additional levels of access.
- Configuration subversion: Improperly configured web servers and application servers are common attack vectors. Agilant Security Solutions assessed the software features, as well as the application and server configuration, for poor configurations.

7.1.2 Common Tools

- Commercially available & open-source tools including, but not limited to: kali Linux, Parrot Os, Blackarch, Nessus, Openvas, Nexpose, Vooki, Arachi, Burp Suite, ZAP proxy, nmap, masscan, ike-scan, Metasploit, ikeprobe, nikto, in-house developed tools, dig, WMIC

8 FINDINGS AND RECOMMENDATIONS

In this section, Agilant details individual infrastructure findings for ACME's Internal Vulnerability assessment. Vulnerabilities are listed in order of importance with critical issues first and low risk issues last. Within each table is the name of the finding, a finding reference number, and the risk rating of the finding. The finding contains a description of the finding, the impact of successful exploitation of the finding, and any sample data or screenshots that accompany the finding. Finally, Agilant suggests recommendations to limit the impact or successful exploitation of the finding.

8.1 Findings

8.1 High Risk Hosts

Synopsis – Hosts included in this section present a significant risk to the environment based upon the number of serious exploitable vulnerabilities discovered.

Due to the sheer volume of information each host listed will have a corresponding supplemental report associated with it outlining the vulnerabilities which should be addresses as soon as possible.

Vulnerability	**Host with more than 5 unique vulnerabilities not covered by any other section**					
Synopsis						
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 0H1	XX.254.11.100	all				
Description						
Host XX.254.11.100 is considered high risk due to the amount of vulnerabilities discovered Please see supplemental document XX.254.11.100.pdf for further details						
Solution						
Additional Resources						
Comments						
See summary of recommendations for additional information						

8.1.1 Anti-Malware and Perimeter

Synopsis – The purpose of this portion of our examine was to evaluate perimeter controls to determine how well devices positioned between the trusted and trusted networks (ie ACME infrastructure and the internet) performed with respect to protecting the internal network from malware, rootkits, botnets & phone home viruses.

While in certain instances the perimeter devices performed well the majority of the time it was possible to circumvent their abilities due to misconfiguration, antiquation and/or lack of capabilities. When examining this fact in a silo the risk rating result for this area would be a critical were it not for the implementation of the Carbon Black endpoint solution.

Vulnerability	**No SSL interception & deep inspection configured at perimeter**					
Synopsis	Our internal to external testing revealed no Intercepting SSL certificate exists					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 1H1	All addresses	HTTPS				
Description						
The vast majority of botent, C&C service communication and malware callbacks are conducted over encrypted SSL channels which can completely bypass IP/content filtering solutions which do not perform deep SSL inspection						
Solution						
Configure SSL interception on all outgoing connections so the firewall/ips can examine SSL encrypted traffic for dangerous traffic patterns. This will require a trusted root certificate and Microsoft PKI ebedded within MS Active Directory						
Additional Resources						
none						
Comments						
This finding would list as a critical without the implementation of Carbon Black on all internal Windows hosts						

Vulnerability	No perimeter blocking of known viruses					
Synopsis	No perimeter device was able to detect viruses which were downloaded into our sandbox environment					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1H2	All addresses	all				
Description						
Several viruses including the famous Eicar test virus were downloaded to our sandboxed laptop as part of the testing. These files made it to the local host over an https encrypted channel and were never intercepted by any inline device. During the insider threat portion of the exam the famous Mimikatz was download via browser and web.client session commandlet without restriction						
Solution						
Configure SSL interception and keep virus signature files up-to-date on perimeter devices						
Additional Resources						
none						
Comments						
This finding would list as a critical without the implementation of Carbon Black on all internal Windows hosts						

Vulnerability	No perimeter blocking of executable content					
Synopsis	Perimeter devices allow the downloading of executable content					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1H3	All addresses	all				
Description						
During the examination a variety of file types including **.exe,.wsh,.ps1,.bat,.com,.scr,.vbs** were downloaded successfully for our sandbox over both http and https methods.						
Solution						
Configure a perimeter device to block executable content and dangerous file types						
Additional Resources						
none						
Comments						
This finding would list as a critical without the implementation of Carbon Black on all internal Windows hosts						

Vulnerability	Unrestricted outbound access					
Synopsis	Egress firewall rules appear to allow any any					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1H4	All addresses	all				
Description						
During the examination our consultants tested outbound communication to our tcp/udp port towers and found all tcp and udp ports are accessible through the firewall. This allows easy access for hackers to establish call back connections to bot net servers and command and control systems which could bypass content inspection tools						
Solution						
Examine business need for all outbound tcp and udp communication and craft rules based upon business need. This is normally done by capturing outbound firewall traffic for a period of 90 days and then building a protocol group for outbound accept firewall rules.						
Additional Resources						
none						
Comments						
This finding would list as a critical without the implementation of Carbon Black on all internal Windows hosts						

Vulnerability	Reverse shells possible over TCP & UDP					
Synopsis	Firewall not fully aware of tcp protocol parameters					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1H5	All addresses	all				
Description						
During our examination our consultants were able to execute reverse shells through the firewall over tcp ports 80 and 443 via Netcat as well as UDP port 123. This reverse shell will bypass the need for a NAT translation and allow full remote control sessions with a minimal footprint much the same way as teamviewer without the need to install software and/or make adjustments to the firewall						
Solution						
Make sure firewall and/or content filter has protocol awareness and configure unknown protocols to generate alerts for further investigation. NGFW (Next Gen Firewalls) such as the Fortigate and Palo Alto have what is known as “APP-ID” for this exact purpose.						
Additional Resources						
none						
Comments						
See summary of recommendations for additional information						

Vulnerability	Reverse shells possible over ICMP					
Synopsis	Unrestricted ICMP access outbound without protocol awareness					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1H6	All addresses	all				
Description						
During our examination our consultants were able to execute reverse tunnels using Hans (**http://code.gerade.org/hans/)** Hans allows for a client side initiated tunnel to be configured through a firewall which allows ICMP to any destination outbound. Once configured the attacker has complete remote control over the client initiator and can use the machine as a jumpbox in further attacks on the network.						
Solution						
Limit outbound ICMP to a few destinations such as 8.8.8.8 and 8.8.4.4 if ICMP and traceroute are troubleshooting tool requirements						
Additional Resources						
none						
Comments						

Vulnerability	No IP address threat intel feeds for egress communication					
Synopsis	Our testing successfully connected to several hosts which exist on several threat intel lists					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1M1			all			
Description						
Our tests revealed there may be no ip blocking lists for known IP addresses configured at the perimeter. We connected successfully to several dozen IP addresses which are well known to at least 4 threat intel lists for distributing malware and/or presenting phishing landing pages						
Solution						
Perimeter devices should include a subscription to threat intel lists which place high risk offenders on permanent block lists						
Additional Resources						
None						
Comments						
See summary of recommendations for additional information						

Vulnerability	Undocumented networks accessible					
Synopsis	Current network documentation does not list all networks which were accessible during our examination					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1M2						
Description						
As part of our kick off discussions our teams requested network IP and VLAN documentation. While we relied on the information included within documents entitled ***Vlans.csv & XXX_VLANS-IP 2020.xlsx*** As a reference point we also conducted our own discovery scan of all RFC1918 address spaces and discovered several dozen networks with hosts that responded to our ping probes. Please see **exhibit A** at the end of this document for a listing of all the networks discovered during this test. This presents a risk to ACME as any vulnerability which exists on an unfirewalled network with a pathway into ACME network is a ACME network risk.						
Solution						
Examine and verify there are no stale VPN tunnels or legacy dedicated lines to networks not accounted for						
Additional Resources						
none						
Comments						
See summary of recommendations for additional information						

Vulnerability	Access to countries considered high attackers					
Synopsis	Outbound communication to Italy was possible from our internal host					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 1M3						
Description						
As part of our testing our consultants attempted to initiate connections to the top countries known for distributing malware **Brazil Iran North Korea Russia China Hungary Italy Romania** Of the countries listed above we were able to successfully connect to hosts in Italy						
Solution						
Consider country blocking Italy in the same manner the other listed countries are being blocked						
Additional Resources						
Comments						
See summary of recommendations for additional information						

Vulnerability	Firewall management pages are accessible from any source					
Synopsis	Access to management protocols on the firewall devices is accessible from all internal hosts					
Severity	**Medium**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 1M4						
Description						
Our testing revealed that firewall management pages was accessible from our testing laptop which was assigned a dynamic ip. From this we can infer that the firewall accepts management connections from any host on the internal network						
Solution						
Configure firewall management acls to limit connections to approved sources only						
Additional Resources						
None						
Comments						
See summary of recommendations for additional information						

8.1.2 Server Network

Synopsis – The purpose of this portion of our examination was to evaluate the settings, patch levels, endpoint protection and hardening techniques which exist on individual servers throughout the network. The overall objective here is to determine if the servers can be easily compromised through a virus attack, Trojan and or targeted protocol attack.

Overall single most effective control protecting the sever network is the implementation of Carbon Black. Without this implementation many of the findings noted in this exam could lead to a full compromise of the entire network should perimeter controls experience a breach or malware gain entry into the network.

As with the malware and perimeter section of this document the implementation of Carbon black brings the risk level on many of findings from a Critical to a high which means the organization is afforded some effective protection but is not utilizing a combined effort, kill chain approach to mitigating risk.

Vulnerability	**Servers not patched in 3 months or more**					
Synopsis	Our testing of server systems revealed a patching program that requires review					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 2H1						
Description						
Our testing through the use of WMI queries and protocol testing revealed a significant lapse in hotfix/security patch application. In many instances servers have not been patched at the Operating system level in over 3 months and are exposed to significant risk should exploit code gain entry to the network. This patching issue persists in both Operating system levels and standard applications such as Internet explorer and Adobe. See **Exhibit 2** for details on servers missing important security updates						
Solution						
ACME should consider an automated enterprise patching solution such as ManageEngine or similar product which is capable of identifying the need and the patching the host at both the operating system and application levels.						
Additional Resources						
None						
Comments						
See summary of recommendations for additional information						

Vulnerability	Unsupported versions of Windows					
Synopsis	Hosts running unsupported versions of Microsoft Windows					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2H2	XXX.168.1.6	all				
Description						
Hosts discovered in this section are running Windows 2003 which is not supported and cannot receive patch updates for known vulnerabilities						
Solution						
Upgrade to supported version of MS windows or place host on an isolated VLAN with additional security controls protecting it from the internet and other hosts as it is deemed a high risk host						
Additional Resources						
None						
Comments						
None						

Vulnerability	HP (OpenView Storage) Data Protector Backup Client Service Directory Traversal					
Synopsis	The IP storage data protector client has a serious flaw in the code which could lead to complete compromise					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2H3	XX.254.20.100	5555				
Description						
The HP storage data protector has a web based vulnerability called a "directory transversal" which enables attackers to escape directory containers within web applications and visit areas of the app not intended for display. This could lead to serious compromise if files are uploaded and executed as part of the attack sequence						
Solution						
Upgrade to a higher version of code following the instructions which can be found here **https://support.hpe.com/hpesc/public/docDisplay?docId=c03822422**						
Additional Resources						
none						
Comments						
None						

Vulnerability	Firebird Default Credentials					
Synopsis	It is possible to connect to the remote database service using default credentials.					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2H4	XX.254.11.225	3050				
Description						
An attacker may use this misconfiguration flaw to execute commands against the remote host, as well as read your database content. The remote Firebird Server uses default credentials (SYSDBA/masterkey)						
Solution						
Change the default password by using the gsec management tool.						
Additional Resources						
http://www.firebirdsql.org/manual/qsg2-config.html#qsg2-config-security						
Comments						
See summary of recommendations for additional information						

Vulnerability	Oracle Java SE Multiple Vulnerabilities					
Synopsis	Outdated version of Oracle java contains multiple vulnerabilities					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2H5	XX.254.11.222 XX.254.190.36					
Description						
Successful exploitation will allow attackers to have an impact on data residing on the server through a variety of exploit mechanisms addressed by the vendor						
Solution						
An enterprise solution such as ManageEngine should be deployed to ensure both operating system and application patches are up to date						
Additional Resources						
http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html						
Comments						
See summary of recommendations for additional information						

Vulnerability	Apache Tomcat Multiple Vulnerabilities					
Synopsis	Apache Tomcat is prone to multiple serious vulnerabilities due to outdated version					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2H6	XX.254.21.14 XX.250.93.16					
Description						
The current version of Tomact is prone to several high risk vulnerabilities as it is significantly outdated						
Solution						
Update to version 7.0.100, 8.5.51, 9.0.31 or later.						
Additional Resources						
https://www.chaitin.cn/en/ghostcat						
Comments						
none						

Vulnerability	Oracle Mysql Security Updates missing					
Synopsis	Mysql database version is unpatched and has several high risk vulnerabilities associated with this version					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2H7	XX.254.190.36	3310				
Description						
Successful exploitation will allow remote attackers to have an impact on the server integrity and any important information which resides on it						
Solution						
Apply latest versions of Mysql						
Additional Resources						
https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html						
Comments						
See summary of recommendations for additional information						

Vulnerability	SMB signing not required					
Synopsis	Signing is not required on the SMB (windows) servers					
Severity	**Medium**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 2M1						

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server

See **Exhibit C** for a listing of affected servers

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing

Additional Resources

https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/cc731957(v=ws.11)?redirectedfrom=MSDN

Comments

See summary of recommendations for additional information

8.1.3 Hypervisor hosts

Synopsis – The purpose of this portion of our examination was to specifically callout hypervisor hosts as they present a greater risk to the organization when vulnerabilities are found as entire disk images along with their information, password hashes etc etc can be offloaded from a server and cracked on an alternate hypervisor in the right set of circumstances.

Overall our evaluation of this system set centers around one serious concern ie SCP and SSH are enabled on at least two ESX hosts. This should be addressed as soon as possible.

Vulnerability	**SSH / SCP accepted from any host**					
Synopsis	Hypervisors accept scp and ssh from any host					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 3H1	XX.254.21.50 XX.254.20.240	22				
Description						
The hypervisors allow SCP and SSH Protocols from any internal source. This could be very dangerous as it may allow for vmdk file downloading and cracking off network						
Solution						
Craft ACLs on the internal layer 3 switching fabric to disallow ssh / scp to the hypervisors						
Additional Resources						
None						
Comments						
None						

8.1.4 Workstations & insider threat

Synopsis – The purpose of this portion of our examination to examine workstations for patch levels, settings, hardening options for end point defense. Through the course of our testing we also sought to discover any instances of malware resident in the processes, startup registry keys, wmi database and scheduled tasks on these workstations. We found none.

Currently workstations are protected through the deployment of Carbon Black which makes their likelihood of compromise considerably lower. There also appears to be strength in policy controls as our testing was unable to reveal ordinary users as administrators of their own workstations.

However, there are items which need to be addressed to ensure a highly robust security posture exists.

Vulnerability	**Windows 7 unpatched hosts**					
Synopsis	Windows 7 which have multiple vulnerabilities related to unapplied patches					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 4H1						
Description						
There are several dozen workstations which remain unpatched and running Windows 7 See **exhibit D**						
Solution						
Upgrade windows 7 hosts to a supported version of Microsoft Windows and deploy an automated patching solution to disseminate patches for Operating systems and applications as they are released by their vendors Please note that several Java, adobe and internet explorer vulnerabilities were found on the same hosts listed on exhibit D which can be addressed through proper patching procedures						
Additional Resources						
None						
Comments						
None						

Vulnerability	Ability to run Macros, Vbscripts and Powershell scripts					
Synopsis	All workstations tested have the ability to run Macros, VBscripts and Powershell					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 4H2						

Description

Workstations have the ability to run Macros, VBscripts and Powershell. These tools are commonly used by attackers to compromise workstations and bypass anti-virus solutions.

Unless absolutely needed for business purposes these tools should be disabled

Solution

To Disable Windows Script Host

Type **regedit** to open the system registry in edit mode.
Navigate to HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\
Create (if it doesn't exist already) a new REG_DWORD key, name it **Enabled** and assign a value of 0 (zero) to it.
Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\
Create (if it doesn't exist already) a new REG_DWORD key, name it **Enabled** and assign a value of 0 (zero) to it.

To disable Macros

https://support.microsoft.com/en-us/office/enable-or-disable-macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

To disable powershell

Windows 10 - https://activedirectorypro.com/disable-powershell-with-group-policy/

Windows 10 / 7 - https://winbuzzer.com/2021/04/28/how-to-disable-powershell-in-windows-10-xcxwbt/

Additional Resources

None

Comments

None

Vulnerability	Lan and wireless cards activated simultaneously					
Synopsis	Wireless card and Lan card both have ip addresses assigned and are enabled					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 4H3						
Description						
Our testing reveal the hosts included in **Exhibit E** had both their Lan cards and Wireless cards active simultaneously with IP addresses assigned. This situation can present a significant risk if an outside attacker is able to jam the wireless signal and force a client to connect to their rogue AP instead of a legitimate one as this now gives them a full entry point into the wired network						
Solution						
Many modern laptops will have an option to disable wireless cards if the Ethernet jack is active (plugged in) http://woshub.com/disable-wi-fi-when-ethernet-cable-connected/						
Additional Resources						
None						
Comments						
None						

Vulnerability	Teamviewer left in a connected and on state					
Synopsis	Teamviewer left running with active outbound connections					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 4H4	XX.254.190.30					
Description						
During our exam we discovered a single host initiating outbound Teamviewer connections during normal business hours and after normal business hours This can be a serious risk to the network as it makes the workstation a jump box into other areas of the network. In the event that credentials are compromised or even the host at the other end of the connection is compromised						
Solution						
Teamviewer should only be used during business hours while support staff are available to review activities. If needed after hours for outside support ACLS should be crafted denying this host access to non-essential areas of the network						
Additional Resources						
None						
Comments						
None						

Vulnerability	Personal email					
Synopsis	Personal email sites such as yahoo & gmail are available					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 4H5						
Description						
Our local endpoint testing revealed access to personal email sites such as yahoo & gmail among others. This can present a risk to the organization as emails sent to these accounts are not filtered according to the policies and profiles of the ACME email filtering system and could be used to circumvent those controls Additionally such sites can be used in a data exfiltration campaign initiated by a rogue employee						
Solution						
Use content filtering and or URL blocking to control access to sites unless needed for business purposes						
Additional Resources						
None						
Comments						
None						

Vulnerability	Personal file storage					
Synopsis	Personal file storage sites are available					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 4H6						
Description						
Our local endpoint testing revealed access to personal file storage sites are available These types of sites can be used in a data exfiltration campaign initiated by a rogue employee and should be highly scrutinized						
Solution						
Use content filtering and or URL blocking to control access to sites unless needed for business purposes						
Additional Resources						
None						
Comments						
None						

Vulnerability	Windows PrintNightmare Registry Exposure					
Synopsis	CVE-2021-34527 OOB Security Update RCE					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 4H7						

Description

A remote command execution vulnerability exists in Windows Print Spooler service improperly performs privileged file operations. An authenticated, remote attacker can exploit this to bypass and run arbitrary code with SYSTEM privileges. The remote system is not fully secure as the point and print registry settings contain an insecure configuration in one of the following locations/keys:

- HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
- HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint\NoWarningNoElevationOnInstall
- HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint\UpdatePromptSettings

Solution

https://support.microsoft.com/en-us/help/5004946

https://support.microsoft.com/en-us/help/5004947

https://support.microsoft.com/en-us/help/5004955

https://support.microsoft.com/en-us/help/5004960

https://support.microsoft.com/en-us/help/5004954

https://support.microsoft.com/en-us/help/5004958

https://support.microsoft.com/en-us/help/5004945

https://support.microsoft.com/en-us/help/5004948

https://support.microsoft.com/en-us/help/5004950

https://support.microsoft.com/en-us/help/5004959

https://support.microsoft.com/en-us/help/5004951

https://support.microsoft.com/en-us/help/5004953

https://support.microsoft.com/en-us/help/5004956

Additional Resources

None

Comments

None

Vulnerability	Microsoft Edge Multiple Vulnerabilities					
Synopsis	Microsoft Edge (Chromium) < 91.0.864.71 Multiple Vulnerabilities					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 4H8						
Description						
The version of Microsoft Edge installed on the remote Windows host is prior to 91.0.864.71. It is, therefore, affected by multiple vulnerabilities as referenced in the July 19, 2021 advisory. See **Exhibit H** for listing of affected hosts						
Solution						
Upgrade to the latest version of edge. Utilize a software and or patch distribution tool such as ManageEngine.						
Additional Resources						
None						
Comments						
None						

Vulnerability	Ability to boot alternate operating system					
Synopsis	Workstations can be booted into alternate operating system via change to bios					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 4H9						
Description						
Our insider threat examination revealed that the BIOS settings are available and unrestricted and allow access to change BOOT sequence parameters. This can be a potential risk if a user wants to circumvent the local controls provided by the deployment of Carbon Black. This situation can also prove useful to an insider who wishes to elevate their own privileges as they can crack the internal SAM database with any one of nearly a dozen Linux distros designed for that very purpose						
Solution						
Set a BIOS password on all local workstations						
Additional Resources						
None						
Comments						
None						

Vulnerability	SMB signing not required					
Synopsis	Signing is not required on the SMB (windows) workstation					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 4M1						
Description						
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB workstation See **Exhibit F** for a listing of affected workstations						
Solution						
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing						
Additional Resources						
https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/cc731957(v=ws.11)?redirectedfrom=MSDN						
Comments						
None						

8.1.5 Networking & Non Windows devices

Synopsis – This section of the examination separated results from the windows section as the hosts discovered were either networking switches/routers/wireless access-points, printers or linux devices

Overall, the two biggest concerns is SNMP public read access is available and much of the networking gear is outdated, EOL life and is no longer supported by the vendor

Vulnerability	**SNMP community string Public**					
Synopsis	Several devices enumerated with the community string "public"					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 5H1						
Description						
Several devices on the Lan allowed read access using the community string public which is a well known default and could lead to further attacks on the host based on the information gathered See **Exhibit I** for a listing of hosts						
Solution						
Change default community string						
Additional Resources						
None						
Comments						
None						

Vulnerability	**Switching devices approaching EOL**					
Synopsis	**HP J9727A 2920** End of Sale announcement					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 5H2						
Description						
Several switches throughout the core infrastructure have an End of Sale announcement date of april 2021. As time passes it will be more and more difficult to RMA failed devices and may be impossible once the device goes end of support in 2022. While Agilant does not recommend swapping out the entire fleet of switches due to this one issue it would be advisable to maintain a spare unit or two in inventory for replacement in the event of failure. Especially given the current supply chain problems experienced throughout the technology vertical						
Solution						
Additional Resources						
None						
Comments						
None						

Vulnerability	Catalyst 2900 series switches					
Synopsis	Unsupported Catalyst switches					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 5H3	XXX.168.6.254 XXX.168.160.1 XXX.168.1.254					

Description

Catalyst 2900 series switch has been end of life since 2016.

In the event of failure it will be impossible to expedite an RMA for this exact switch and newer models will not allow for the version of code currently running.

To avoid prolonged outages in the event of failure ACME should consider the investment into one similarly modeled switch and test the existing configuration transported from one of these outdated models to the new one. This can serve as a viable alternative to upgrading all the switches while still ensuring the speedy recovery in the event of failure.

Solution

Additional Resources

None

Comments

None

Vulnerability	Catalyst 3750E series switches					
Synopsis	Unsupported Catalyst switches					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 5H4	XXX.168.1.253 XXX.168.99.253					
Description						
Catalyst 3750E series switch has been end of life since 2012. In the event of failure it will be impossible to expedite an RMA for this exact switch and newer models will not allow for the version of code currently running. To avoid prolonged outages in the event of failure ACME should consider the investment into one similarly modeled switch and test the existing configuration transported from one of these outdated models to the new one. This can serve as a viable alternative to upgrading all the switches while still ensuring the speedy recovery in the event of failure.						
Solution						
Additional Resources						
None						
Comments						
None						

Vulnerability	FTP Brute Force Logins Reporting					
Synopsis	FTP credentials easily compromised					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 5H5	XX.254.171.196	21				
Description						
It was possible to login with the following credentials <User>:<Password> **root:root**						
Solution						
Change password as soon as possible						
Additional Resources						
None						
Comments						
None						

Vulnerability	SSH Brute Force					
Synopsis	SSH Brute Force Logins With Default Credentials Reporting					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 5H6						
Description						
It was possible to login with the following credentials <User>:<Password> **root:calvin**						
Solution						
Change root password as soon as possible						
Additional Resources						
None						
Comments						
None						

Vulnerability	SNMP Write access enabled					
Synopsis	SNMP write access enabled					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 5M1						
Description						
All hosts listed in **Exhibit K** allow write access via snmp						
Solution						
ACL access to snmp port 161/UDP, disable write access or configure a highly complex community string						
Additional Resources						
none						
Comments						
None						

8.1.6 Wireless assessment

Synopsis – This section of the examination focused entirely on the access points distributed throughout the network. Overall no findings were noted as we were only able to obtain the hidden SSID but no pre-shared keys

9 RISK ASSESSMENT MATRIX

Vulnerability	Likelihood	Impact	Asset	Mitigating Control	Mitigating Control Effectiveness	Residual Risk
Malware infection and network compromise	High	High	Computer network & hosts ,	Firewall & IPS Carbon Black	Sub-optimal effective	Medium
Ransomware	Medium	High	Computer network & hosts ,	Firewall & IPS Carbon Black	Sub-optimal effective	Medium
Remote control Trojans	High	Medium	Computer network & hosts	Firewall & IPS Carbon Black	Sub-optimal effective	High
Data Exfiltration	Medium	High	Privacy data on employees, cases and individuals	Firewall	Sub-optimal	High
Bandwidth saturation DOS attack	Medium-	Medium	Outside access	Firewall & IPS	Sub-optimal	High
Targeted service attack on hosts conducted via tcp/udp	Medium	Medium	Computer network & hosts	none	ineffective	Medium
Network device failure	Medium	high	Computer network and system access	none	ineffective	Medium

10 RECOMMENDATION PRIORITIZATION

Upon completion of our risk and vulnerability evaluation our consultants determined that a large majority of the internal risks can be mitigated through investments in Newer more robust perimeter defenses which are used to the apex of their potential, the deployment of an enterprise patching solution and the implementation of GPO polices to control access to application and configure advanced settings on the hosts.

1. As outlined in the external report device consolidation and upgrade is a key risk mitigation strategy
2. Egress communication has to be evaluated thoroughly over a adequate amount of time to determine which services are business critical so that appropriate firewall rules can be configured
3. Advanced features designed to understand the deep mechanics of various protocols should be leveraged to avoid protocol spoofing
4. Threat protection services such as Threat intel lists, anti-malware services, IPS, sandboxing and url filtering such be deployed with a NGFW set to improve the perimeter defense barrier
5. An independent management network for device management access should be configured and partitioned in such a way that only the IT staff can access it
6. Tripwire rules should be configured on the firewall which generate email alerts to administrators in the event certain events indicative of compromise are recorded
7. SSL interception & inspection of all outgoing traffic must be configured.
8. Access to highly charged areas of the world should be closely monitored and re-evaluated regularly for appropriateness
9. A spare unit of aging networking equipment should be preemptively purposed and provisioned in a test environment with existing configurations to ensure they are capable of complete compatibility with existing device demands via the command instructions provided
10. A review of the entire network layout as compared to internal documentation should be performed. Device discovery tools should be used to regularly determine what is attached to the LAN.
11. New deployments of servers should pay close attention to remote access cards such as ILOs and Dracs as these often allow complete remote access to the server and are factory shipped with default credentials
12. Non windows and linux based systems should be considered for AD integration via the LDAP protocol so that password history, lockout and complexity requirements persist
13. Unsupported versions of windows including Server 2003 and 2008 and windows 7 workstations should be considered a risk and partitioned into a separate VLAN until resources allow for upgrades
14. GPOs should be deployed to configure Macro access, PowerShell, AppLocker, windows scripting host and operating system level parameters such as restrict anonymous and SMB signing among others.
15. Local device hardware should be secured with the use of a BIOS password to avoid local tampering and escalation of privilege.

11 EXHIBITS

Exhibit A

XX.XX.28.0	XX.140.0.0	XX.140.1.0
XX.140.2.0	XX.140.3.0	XX.15.15.0
XX.20.101.0	XX.20.12.0	XX.252.0.0
XX.254.11.0	XX.254.111.0	XX.254.152.0
XX.254.166.0	XX.254.169.0	XX.254.17.0
XX.254.18.0	XX.254.19.0	XX.254.191.0
XX.254.20.0	XX.254.21.0	XX.254.216.0
XX.254.217.0	XX.254.218.0	XX.254.219.0
XX.254.22.0	XX.254.220.0	XX.254.221.0
XX.254.23.0	XX.254.24.0	XX.254.25.0
XX.254.253.0	XX.254.255.0	XX.254.26.0
XX.254.27.0	XX.254.3.0	XX.254.36.0
XX.254.37.0	XX.254.71.0	XX.254.73.0
XX.254.75.0	XX.51.1.0	1XX.16.XX.0
1XX.16.30.0	1XX.16.5.0	1XX.16.50.0
1XX.16.6.0	1XX.19.0.0	XXX.168.0.0
XXX.168.111.0	XXX.168.128.0	XXX.168.130.0
XXX.168.150.0	XXX.168.160.0	XXX.168.19.0
XXX.168.200.0	XXX.168.207.0	XXX.168.21.0
XXX.168.220.0	XXX.168.240.0	XXX.168.245.0
XXX.168.27.0	XXX.168.34.0	XXX.168.37.0
XXX.168.50.0	XXX.168.51.0	XXX.168.55.0
XXX.168.6.0	XXX.168.70.0	XXX.168.99.0

Exhibit B

XX.XX.28.120	XX.XX.28.161	XX.XX.28.162
XX.XX.28.171	XX.XX.28.172	XX.XX.28.2
XX.XX.28.3	XX.140.1.164	XX.15.15.81
XX.15.15.83	XX.250.93.16	XX.254.11.101
XX.254.11.111	XX.254.11.114	XX.254.11.225
XX.254.11.4	XX.254.11.40	XX.254.11.5
XX.254.11.60	XX.254.11.68	XX.254.11.7
XX.254.190.17	XX.254.190.36	XX.254.20.100
XX.254.20.110	XX.254.20.112	XX.254.20.115
XX.254.20.64	XX.254.20.71	XX.254.20.72
XX.254.20.73	XX.254.21.14	XX.254.21.44
XX.254.40.31	1XX.19.0.240	1XX.19.0.246
1XX.19.0.251	XXX.168.0.144	XXX.168.1.6
XXX.168.1.8	XXX.168.200.204	XXX.168.200.219
XXX.168.200.225	XXX.168.200.23	XXX.168.200.47
XXX.168.51.6	XXX.168.55.11	XXX.168.55.13
XXX.168.55.250	XXX.168.6.19	

Exhibit C

XX.XX.28.120	XX.140.1.164	XX.15.15.81
XX.254.11.101	XX.254.11.108	XX.254.11.111
XX.254.11.114	XX.254.11.130	XX.254.11.131
XX.254.11.152	XX.254.11.171	XX.254.11.200
XX.254.11.217	XX.254.11.222	XX.254.11.225
XX.254.11.4	XX.254.11.40	XX.254.11.60
XX.254.11.68	XX.254.11.69	XX.254.11.7
XX.254.11.8	XX.254.11.86	XX.254.11.87
XX.254.11.9	XX.254.190.17	XX.254.190.36
XX.254.20.100	XX.254.20.110	XX.254.20.200
XX.254.20.23	XX.254.20.64	XX.254.20.71
XX.254.20.72	XX.254.20.73	XX.254.21.140
XX.254.21.44	XX.254.21.99	XX.254.40.31
1XX.19.0.251	XXX.168.1.6	XXX.168.1.8
XXX.168.200.219	XXX.168.200.225	XXX.168.200.23
XXX.168.200.47	XXX.168.55.11	XXX.168.55.250
XXX.168.6.19		

Exhibit D

XX.254.221.128	XX.254.30.103	XX.254.30.55
XX.254.70.103	XX.254.70.104	XX.254.70.110
XX.254.70.115	XX.254.70.122	XX.254.70.125
XX.254.70.127	XX.254.70.131	XX.254.70.50
XX.254.70.51	XX.254.70.52	XX.254.70.54
XX.254.70.59	XX.254.70.64	XX.254.70.69
XX.254.70.86	XX.254.70.89	XX.254.70.90
XX.254.70.91	XX.254.70.94	XX.254.70.95
XX.254.70.96	XX.254.70.97	XX.254.70.98
XXX.168.12.123	XXX.168.13.70	XXX.168.21.11
XXX.168.30.77		

Exhibit E

XX.254.216.115	XX.254.216.235	XX.254.216.33
XX.254.216.35	XX.254.216.40	XX.254.216.66
XX.254.216.80	XX.254.218.247	XX.254.218.32
XX.254.218.60	XX.254.219.199	XX.254.219.37
XX.254.219.40	XX.254.220.156	XX.254.220.159
XX.254.220.194	XX.254.220.212	XX.254.220.87
XX.254.220.88	XX.254.220.91	XX.254.221.105
XX.254.221.128	XX.254.221.138	XX.254.221.225
XX.254.27.38	XXX.168.21.11	

Exhibit F

XX.254.11.100	XX.254.11.131	XX.254.120.98
XX.254.15.155	XX.254.15.176	XX.254.15.185
XX.254.15.186	XX.254.15.189	XX.254.160.105
XX.254.160.141	XX.254.160.142	XX.254.160.144
XX.254.160.145	XX.254.160.146	XX.254.170.113
XX.254.170.143	XX.254.170.26	XX.254.170.28
XX.254.170.35	XX.254.190.30	XX.254.21.150
XX.254.216.109	XX.254.216.113	XX.254.216.115
XX.254.216.33	XX.254.216.40	XX.254.216.66
XX.254.216.80	XX.254.216.93	XX.254.217.197
XX.254.21.74	XX.254.218.32	XX.254.218.60
XX.254.21.87	XX.254.219.151	XX.254.21.92
XX.254.219.216	XX.254.219.37	XX.254.219.40
XX.254.21.95	XX.254.219.8	XX.254.220.100
XX.254.220.156	XX.254.220.179	XX.254.220.194
XX.254.220.212	XX.254.220.87	XX.254.220.88
XX.254.220.91	XX.254.221.128	XX.254.221.138
XX.254.221.225	XX.254.27.38	XX.254.30.61
XX.254.30.98	XX.254.3.117	XX.254.3.122
XX.254.36.147	XX.254.36.156	XX.254.36.164
XX.254.36.167	XX.254.36.171	XX.254.36.183
XX.254.3.66	XX.254.36.75	XX.254.37.65
XX.254.37.71	XX.254.40.115	XX.254.40.15
XX.254.40.20	XX.254.40.27	XX.254.40.42
XX.254.40.63	XX.254.40.91	XX.254.40.96
XX.254.55.70	XX.254.70.100	XX.254.70.101
XX.254.70.103	XX.254.70.105	XX.254.70.109
XX.254.70.121	XX.254.70.126	XX.254.70.127
XX.254.70.129	XX.254.70.131	XX.254.70.133
XX.254.70.51	XX.254.70.53	XX.254.70.55
XX.254.70.57	XX.254.70.60	XX.254.70.62
XX.254.70.63	XX.254.70.65	XX.254.70.66
XX.254.70.67	XX.254.70.68	XX.254.70.69
XX.254.70.70	XX.254.70.71	XX.254.70.73
XX.254.70.77	XX.254.70.79	XX.254.70.80
XX.254.70.83	XX.254.70.84	XX.254.70.85
XX.254.70.87	XX.254.70.92	XX.254.70.93
XX.254.70.96	XX.254.70.99	XX.254.80.58
XXX.168.111.4	XXX.168.111.56	XXX.168.12.60
XXX.168.13.133	XXX.168.13.143	XXX.168.17.40
XXX.168.18.254	XXX.168.18.40	XXX.168.20.40
XXX.168.20.67	XXX.168.21.11	XXX.168.21.69
XXX.168.22.74	XXX.168.22.94	XXX.168.24.40
XXX.168.29.40	XXX.168.30.40	XXX.168.30.77
XXX.168.4.108	XXX.168.4.39	XXX.168.44.40
XXX.168.5.38	XXX.168.7.40	XXX.168.82.40

Exhibit G

XX.254.15.176	XX.254.15.185	XX.254.15.189
XX.254.170.26	XX.254.216.115	XX.254.219.216
XX.254.220.91	XX.254.221.128	XX.254.30.103
XX.254.30.55	XX.254.36.164	XX.254.37.71
XX.254.70.103	XX.254.70.104	XX.254.70.110
XX.254.70.122	XX.254.70.125	XX.254.70.127
XX.254.70.131	XX.254.70.50	XX.254.70.51
XX.254.70.52	XX.254.70.54	XX.254.70.59
XX.254.70.62	XX.254.70.69	XX.254.70.70
XX.254.70.86	XX.254.70.89	XX.254.70.90
XX.254.70.91	XX.254.70.94	XX.254.70.95
XX.254.70.96	XX.254.70.97	XX.254.70.98
XXX.168.12.123	XXX.168.13.70	XXX.168.17.40
XXX.168.18.40	XXX.168.20.40	XXX.168.21.11
XXX.168.24.40	XXX.168.29.40	XXX.168.30.40
XXX.168.30.77	XXX.168.4.39	XXX.168.44.40
XXX.168.5.38	XXX.168.7.40	XXX.168.82.40

Exhibit H

XX.254.15.176	XX.254.15.185	XX.254.15.189
XX.254.170.26	XX.254.216.115	XX.254.219.216
XX.254.220.91	XX.254.221.128	XX.254.30.103
XX.254.30.55	XX.254.37.71	XX.254.70.103
XX.254.70.104	XX.254.70.110	XX.254.70.122
XX.254.70.125	XX.254.70.127	XX.254.70.131
XX.254.70.50	XX.254.70.51	XX.254.70.54
XX.254.70.59	XX.254.70.62	XX.254.70.69
XX.254.70.70	XX.254.70.86	XX.254.70.90
XX.254.70.91	XX.254.70.94	XX.254.70.95
XX.254.70.96	XX.254.70.97	XX.254.70.98
XXX.168.12.123	XXX.168.13.70	XXX.168.17.40
XXX.168.18.40	XXX.168.20.40	XXX.168.21.11
XXX.168.21.69	XXX.168.24.40	XXX.168.29.40
XXX.168.30.40	XXX.168.30.77	XXX.168.4.39
XXX.168.44.40	XXX.168.5.38	XXX.168.7.40
XXX.168.82.40		

Exhibit I

XX.XX.28.132	XX.XX.28.133	XX.XX.28.146
XX.XX.28.147	XX.XX.28.148	XX.XX.28.149
XX.XX.28.160	XX.XX.28.170	XX.15.15.31
XX.15.15.59	XX.15.15.9	XX.15.15.62
XX.15.15.150	XX.15.15.151	XX.15.15.152
XX.15.15.153	XX.140.1.85	XX.254.3.201
XX.254.3.202	XX.254.3.203	XX.254.3.231
XX.254.3.232	XX.254.3.240	XX.254.3.241
XX.254.3.242	XX.254.3.243	XX.254.3.244
XX.254.3.246	XX.254.3.248	XX.254.3.249
XX.254.3.250	XX.254.11.16	XX.254.11.228
XX.254.12.241	XX.254.12.242	XX.254.12.245
XX.254.16.239	XX.254.16.240	XX.254.16.245

Exhibit J

	XX.XX.28.132	XX.XX.28.133
XX.XX.28.146	XX.XX.28.147	XX.XX.28.148
XX.XX.28.149	XX.XX.28.160	XX.XX.28.170
XX.15.15.31	XX.15.15.59	XX.15.15.9
XX.15.15.62	XX.15.15.150	XX.15.15.151
XX.15.15.152	XX.15.15.153	XX.140.1.85
XX.254.3.201	XX.254.3.202	XX.254.3.203