REPORT

ACME Test Industries
External Vulnerability Assessment Report

August 7, 2021

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 initial phase was comprised of a blind Outside Vulnerability Assessment, which was both conducted and concluded. This report describes its results, the methodology employed, the overall risk to the organization, the effectiveness of the components tested, and our overall observations. This report also provides recommendations for next steps in mitigating risk through configuration changes and/or technology investments, where appropriate.

Speaking to the outside perimeter of ACME's computer network, a significant investment has been made in security-related technologies. These systems are dedicated to the task of protecting the organization from threats targeting publicly accessible web & application servers. However, despite this investment, many of the devices are aging, unsupported by their respective vendors, and/or are configured sub-optimally to produce the intended effect.

The most significant examples of sub-optimal configuration are related to the inline IPS, VPN devices, firewall, and related SIEM solution. These components, working together, should allow for an automated and effective approach in blocking remote attacks. But in certain situations, they do not. In others, they provide the security analyst with information that is hard-to-examine, and sometimes obfuscated.

Additional findings, as noted in future sections, relate to aging hardware & software, common oversights, and natural vulnerability lifecycles existent in all major software platforms as products undergo constant scrutiny by threat actors.

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 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 engaged Agilant to conduct a comprehensive vulnerability assessment consisting of several components. To provide the best possible service to ACME, Agilant has constructed the overall report in "chunks" in the hopes of making the information easier to digest 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 Outside Vulnerability Assessment: Agilant consultants enumerated and reviewed all publicly accessible hosts as they appear on the internet. A full network profile was constructed 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 (as the first of a series): Agilant prepared a document to detail findings and recommendations of the 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.

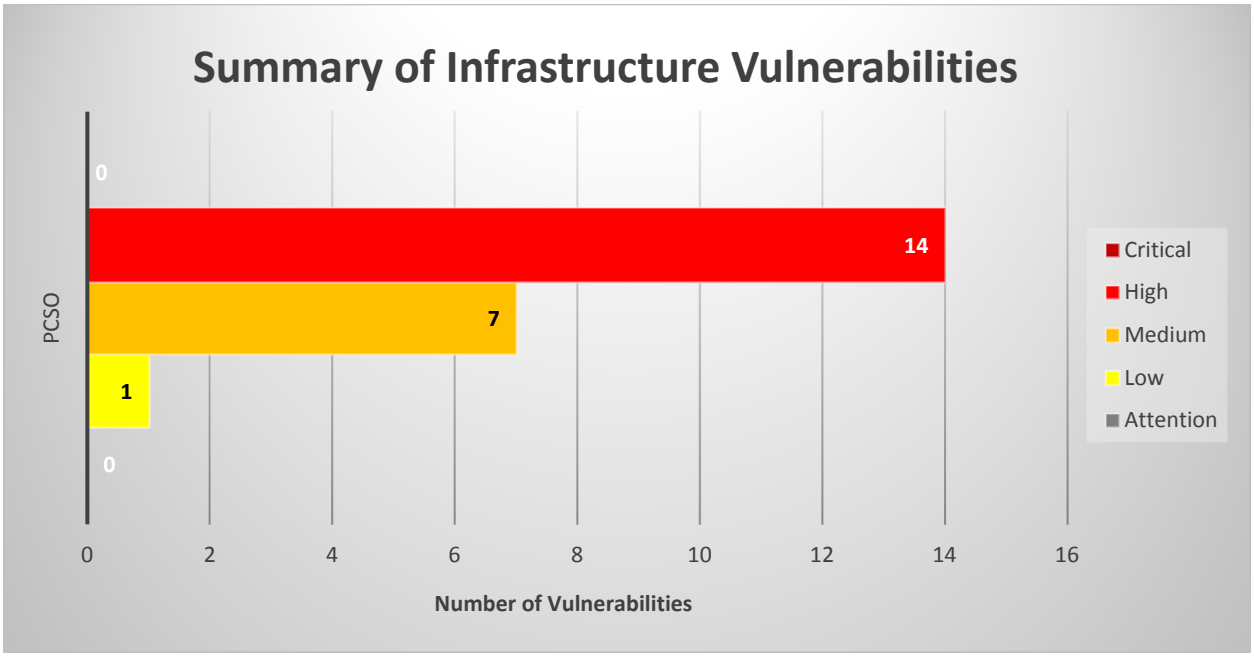
6 CONSOLIDATED SUMMARY OF FINDINGS

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
- Device/software version
- Device/software support & age
- Patch Management
- Encryption

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,

8 FINDINGS AND RECOMMENDATIONS

In this section, Agilant details individual infrastructure findings for ACME's External 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 High Risk Findings

8.1.1 Operational Risk Findings

Vulnerability	**IPS System Blinded by Encrypted Connections**					
Synopsis	Encrypting http traffic to web servers renders the inline IPS system unable to view the attacks and is therefore inoperable in this circumstance					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 1HO	All addresses	HTTPS				
Description						
During the targeted web vulnerability assessment portion of the engagement where we specifically isolated publically accessible web hosts for deep vulnerability analysis over the HTTP protocol we observed an inline IPS system captured our attack traffic, recorded our offending IP address and blocked further connections. However, when performing the exact same attack patterns over the HTTPS protocol the inline IPS system was unable to perform the same functions. We believe this is due to client to server encryption employed during this phase of the attack.						
Solution						
Configure SSL interception on incoming HTTPS traffic destined to web servers						
Additional Resources						
Comments						
See summary of recommendations for additional information						

Vulnerability	No IPS or External Alerting System For Outside Perimeter					
Synopsis	IPS system did not capture traffic that was targeting hosts between the outside firewall interface and the internet router					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2HO	All addresses	all				
Description						
During the initial stages of the outside vulnerability assessment our team performed several reconnaissance scans which were performed in such a way as to set off alarms on any capable firewall or IDS/IPS system. In addition to this we also ran broad sweeps using attack tools and observed there were no alerts generated for our activity when directing attacks at hosts with no inbound network address translations.						
Solution						
Configure anti recon measures on outside interfaces of all publicly accessible systems such as border routers, firewalls, VPNs etc.						
Additional Resources						
Comments						
See summary of recommendations for additional information						

Vulnerability	IPS System Obfuscates Critical Information					
Synopsis	System generated alerts obfuscate critical information					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 3HO	All addresses	all				
Description						
During the unencrypted phases of the outside test log files were requested to examine what type of output is being provided to security analysts from both the SIEM solution and reporting devices. Upon examination it was determined that information on directionality of packets is not obvious to the observer nor is there complete information contained within the fields. In many instances packets appear to be coming from a single source address which is certainly a NAT address thereby obfuscating the true source.						
Solution						
Additional Resources						
Comments						
See summary of recommendations for additional information						

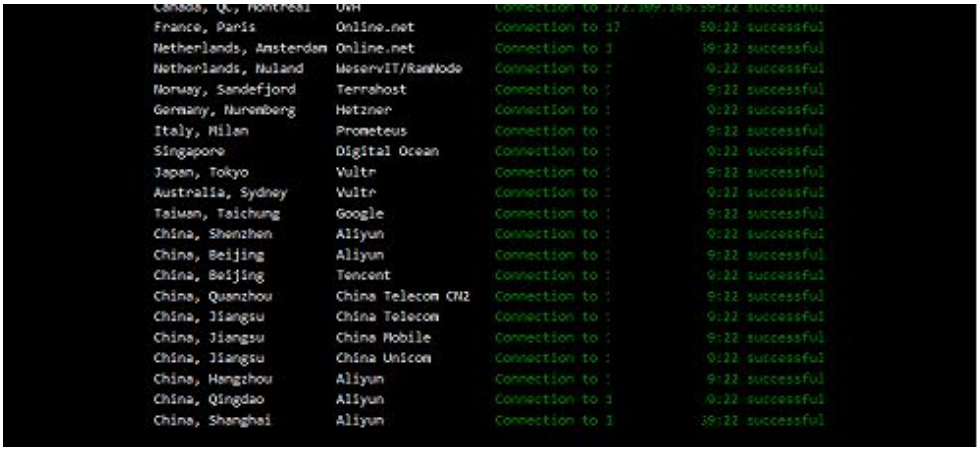
Vulnerability	SIEM Solution is Overwhelmed with Incoming Data					
Synopsis	SIEM solution is recording data in a single dataset for a multitude of devices					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 4HO	All addresses	all				
Description						
During the examination our consultants observed that it was difficult for the analysts to extract precise information for specific devices from the SIEM solution. A SIEM solution which does not make the job of mining for critical events easier and more expeditious is considered a sub performing technology.						
Solution						
Isolate perimeter devices and those that are tasked with examining the behavior of egress and ingress traffic from the operational data such as user logins						
Additional Resources						
Comments						
See summary of recommendations for additional information						

8.1.2 Technology-Based Findings

Vulnerability	SSH Available from Any Source					
Synopsis	SSH connections to host can be established from any source					
Severity	High					
CVSS Score	0	CVE			Exploitable	Yes
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 5HT	xxx.xxx.145.59	22				

Description

The remote server accepts SSH logins from any source.



Solution

At the border router or firewall ACME should restrict incoming connections to this system to those areas where there is a higher degree of trust. Connections from around the world should be limited to only sources deemed critical to the function of the operation.

Additional Resources

Comments

Vulnerability	No Countermeasures for Brute Forcing SSH Accounts Exist					
Synopsis	Brute Forcing high access accounts is possible					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 6HT	xxx.xxx.145.59	22				

Description

The remote server does not have any brute force countermeasures such as IP blocking during a brute force attack against root, admin or administrator.

Normally scanners run brute force attacks at the rate of 36 tries per minute which means an attack using the readily available "rockyou" wordlist which contains 15,000,000 entries could be competed against privileged accounts (which normally do not lock out) in less than a year.

Without an alerting or automatic blocking mechanism in place it is only a matter of time before highly privileged accounts are compromised

Solution

Allow only approved source IP addresses to access ssh. Implement ssh brute force countermeasures on SSH protocol such as successive retry delays, account lockout over the network on privileged accounts and connection throttling

Additional Resources

Comments

Vulnerability	HTTP Request Smuggling					
Synopsis						
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 7HT	xxx.xxx.37.166	443	SSL			

Description

HTTP request smuggling vulnerabilities arise when websites route HTTP requests through webservers with inconsistent HTTP parsing.

By supplying a request that gets interpreted as being different lengths by different servers, an attacker can poison the back-end TCP/TLS socket and prepend arbitrary data to the next request. Depending on the website's functionality, this can be used to bypass front-end security rules, access internal systems, poison web caches, and launch assorted attacks on users who are actively browsing the site.

Solution

Follow the instructions found here: https://msrc.microsoft.com/update-guide/vulnerability/ADV200008

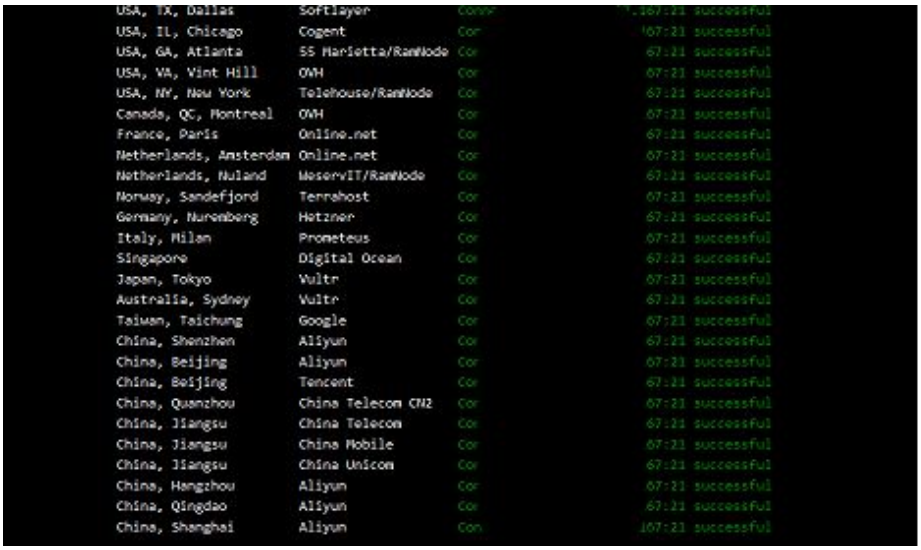
Additional Resources

Comments

Vulnerability	FTP Is Available for All Sources & Is An Unencrypted File Transferring Protocol					
Synopsis	Unencrypted File Transfer Protocol open to all sources					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 8HT	xxx.xxx.37.167	21	FTP			

Description

Server accepting incoming connections over clear text from any source.



Solution

At the border router or firewall ACME should restrict incoming connections to this system to those areas where there is a higher degree of trust. Connections from around the world should be limited to only sources deemed critical to the function of the operation

Additional Resources

Comments

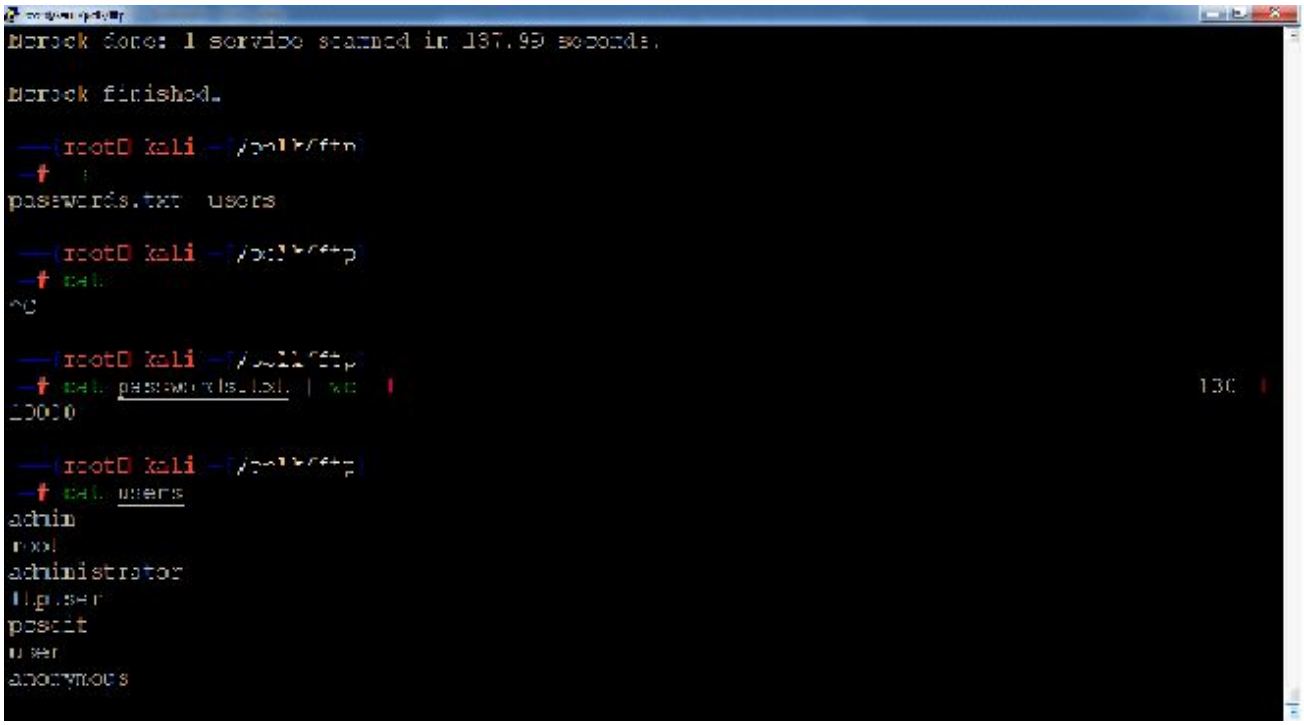
See summary of recommendations for additional information

Vulnerability	No Countermeasures for FTP Brute Force Appear to Exist					
Synopsis	Brute force cracking of credentials may be possible					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 9HT	xxx.xxx.37.167	21	FTP			

Description

Our consultants attempted a brute force cracking campaign against this FTP leveraging a word list with 10,000 entries per username and a file with 7 unique usernames. This campaign should have generated enough attempts that any inline IPS system or host-based firewall should have blocked the offending IP address & produced an alert.

We were able to successfully reconnect with the same source upon competition of the campaign.



Solution

At the border router or firewall ACME should restrict incoming connections to this system to those areas where there is a higher degree of trust. Connections from around the world should be limited to only sources deemed critical to the function of the operation

Additional Resources

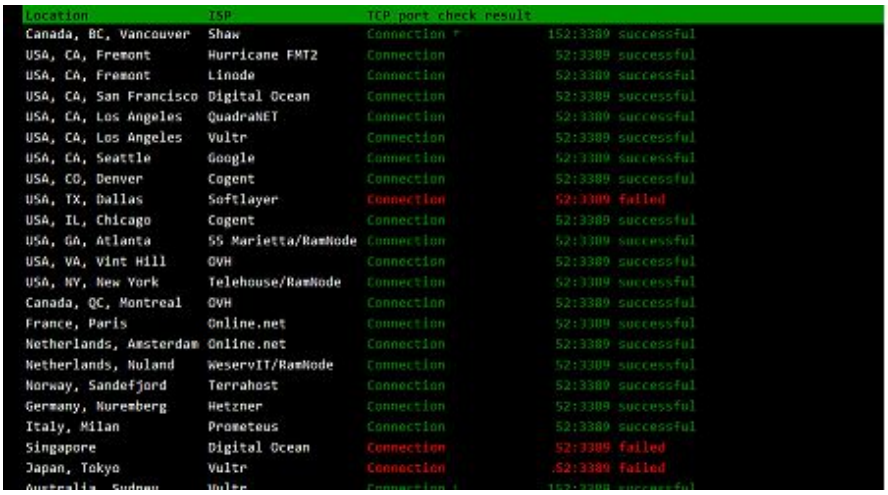
Comments

See summary of recommendations for additional information

Vulnerability	MS RDP Protocol Is Available from All Sources					
Synopsis	A remote access protocol is available from any public source					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 10HT	xxx.xxx.6.152	all				

Description

The Microsoft remote access protocol is available from all sources. This is a potentially dangerous situation as there are several vulnerabilities which exist that can allow a full compromise of the affected host.



Location	ISP	TCP port check result
Canada, BC, Vancouver	Shaw	Connection to 152:3389 successful
USA, CA, Fremont	Hurricane FMT2	Connection 52:3389 successful
USA, CA, Fremont	Linode	Connection 52:3389 successful
USA, CA, San Francisco	Digital Ocean	Connection 52:3389 successful
USA, CA, Los Angeles	QuadraNET	Connection 52:3389 successful
USA, CA, Los Angeles	Vultr	Connection 52:3389 successful
USA, CA, Seattle	Google	Connection 52:3389 successful
USA, CO, Denver	Cogent	Connection 52:3389 successful
USA, TX, Dallas	Softlayer	Connection 52:3389 failed
USA, IL, Chicago	Cogent	Connection 52:3389 successful
USA, GA, Atlanta	SS Marietta/RamNode	Connection 52:3389 successful
USA, VA, Vint Hill	OVH	Connection 52:3389 successful
USA, NY, New York	Telehouse/RamNode	Connection 52:3389 successful
Canada, QC, Montreal	OVH	Connection 52:3389 successful
France, Paris	Online.net	Connection 52:3389 successful
Netherlands, Amsterdam	Online.net	Connection 52:3389 successful
Netherlands, Nuland	WeservIT/RamNode	Connection 52:3389 successful
Norway, Sandefjord	Terrahost	Connection 52:3389 successful
Germany, Nuremberg	Hetzner	Connection 52:3389 successful
Italy, Milan	Prometeus	Connection 52:3389 successful
Singapore	Digital Ocean	Connection 52:3389 failed
Japan, Tokyo	Vultr	Connection 52:3389 failed
Australia, Sydney	Vultr	Connection 152:3389 successful

Solution

Restrict access to the RDP protocol to approved sources

Additional Resources

Comments

Vulnerability	Cross Site Scripting (reflected)					
Synopsis	XSS vulnerability exists on website					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 11HT	xxx.xxx.37.166	443	SSL	.org		
Description						
Solution						
Implement a commercial or open source WAF Open source: https://www.aqtronix.com/?PageID=114 https://geekflare.com/webknight-iis-waf/ <- instructions Enterprise: https://www.imperva.com/products/web-application-firewall-waf/ **Evaluate need for continued availability to the public:** Based on the existence of an expired certificate and verbiage on the site which indicates it may be a stale web site it may be advisable to remove this server entirely						
Additional Resources						
Comments						
See summary of recommendations for additional information						

Vulnerability	IKE VPN using highly vulnerable version of software which is end of support					
Synopsis	The IKE protocol which is used for VPN access contains multiple vulnerabilities					
Severity	High					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 12HT	xxx.xxx.6.153	UDP 500	IKE			

Description

The version of software running on this VPN device was first released in 2005. It is now end of life and end of support and contains multiple vulnerabilities including those listed here

https://www.cisco.com/c/dam/en/us/support/docs/csa/cisco-sa-20130410-asa.html
https://nvd.nist.gov/vuln/detail/CVE-2008-3815
https://www.networkworld.com/article/3121580/cisco-discloses-pix-firewall-ios-software-security-holes.html
https://vulmon.com/searchpage?page=1&q=Cisco+Pix+Security+Appliance+7.0&sortby=byrelevance&scoretype=cvssv3

```
└─# ike-scan -M --showbackoff 65.217.6.153
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/
)
        .153    Main Mode Handshake returned
        HDR=(CKY-R=406232d4c9a5f98c)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Secon
ration=28800)
        VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentatior

IKE Backoff Patterns:

IP Address      No.     Recv time               Delta Time
f  ...  6.153   1       1626554498.568524       0.000000
        6.153   2       1626554506.565660       7.997136
        6.153   3       1626554514.565649       7.999989
        6.153   4       1626554522.565599       7.999950
        6.153   Implementation guess: Cisco VPN Concentrator or PIX 7.0
```

Solution

Additional Resources

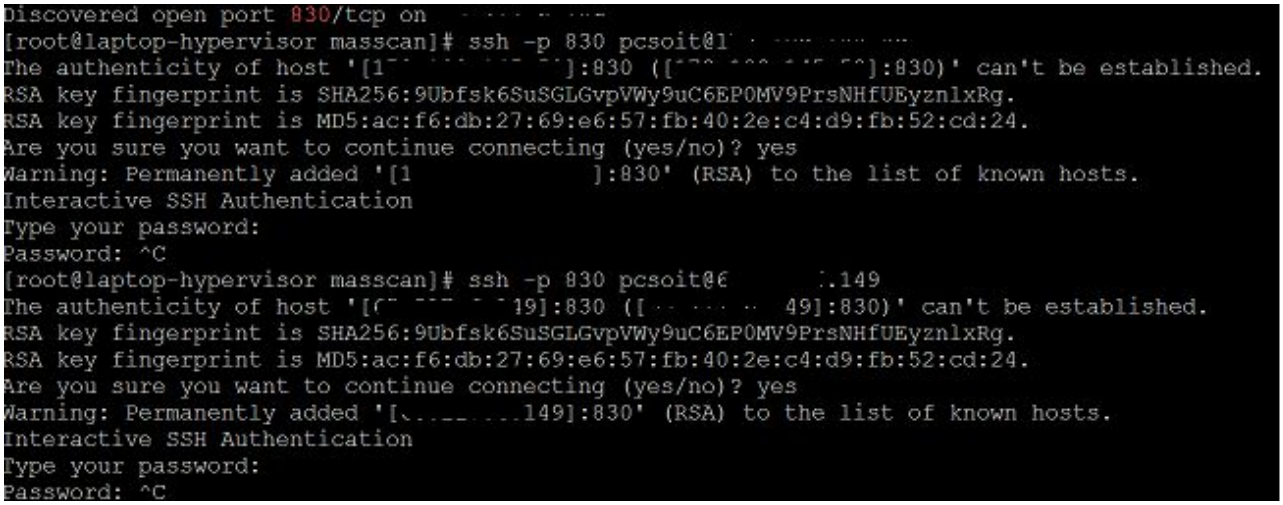
Comments

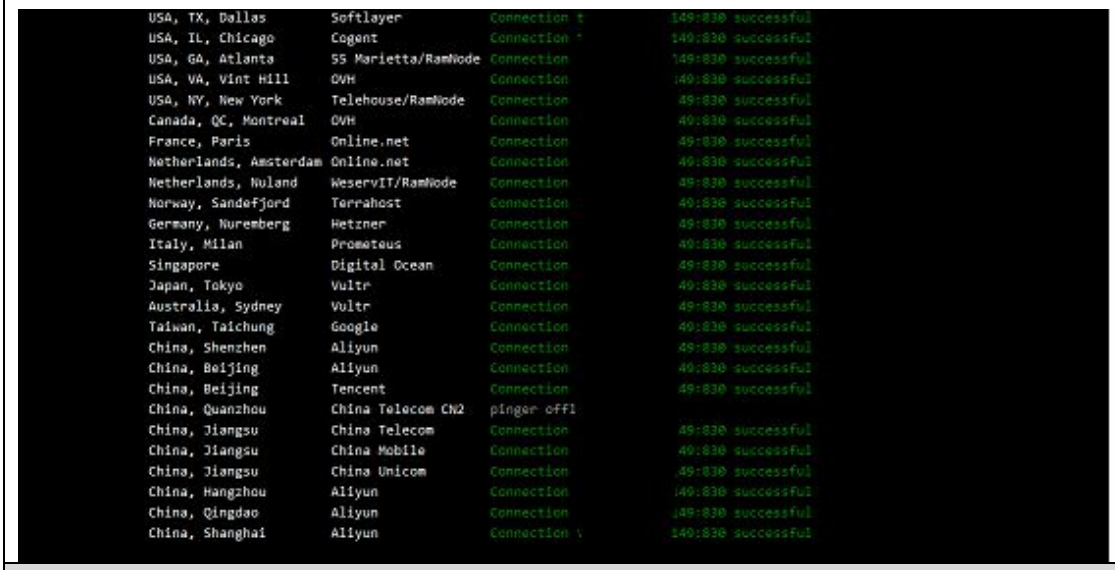
See summary of recommendations for additional information

Vulnerability	SSH NETCONF Open to Public From Any Source					
Synopsis	Brute Forcing high access accounts is possible					
Severity	HIgh					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 13HT	xxx.xxx.145.59 xxx.xxx.6.149	830				

Description

The remote server appears to be an IOS based device which is accepting incoming ssh sessions over tcp port 830 from any source.





Solution

Allow only approved source IP addresses to access ssh.

Additional Resources

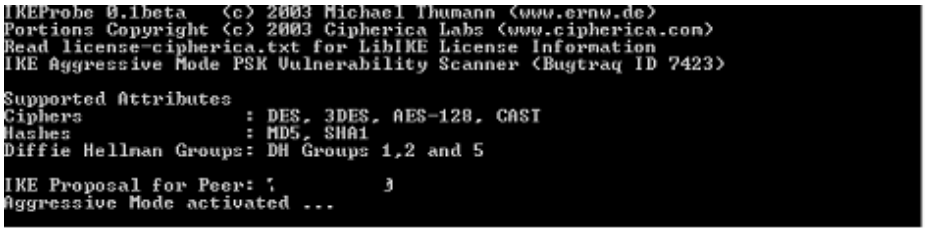
Comments						
Vulnerability	**Host Appears to Be Unprotected By Firewall**					
Synopsis	Publicly accessible host is listening on all ports common to a MS Windows Server					
Severity	**High**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 14HT	xxx.xxx.6.152	Screen shot	Screen shot			
Description						

```
PORT      STATE    SERVICE          VERSION
22/tcp    filtered ssh
23/tcp    filtered telnet
135/tcp   open     msrpc?
139/tcp   open     netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
3389/tcp  open     ms-wbt-server?
5009/tcp  open     airport-admin?
5010/tcp  open     telelpathstart?
5985/tcp  open     http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open     http-proxy
47001/tcp open     http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open     msrpc            Microsoft Windows RPC
49665/tcp open     msrpc            Microsoft Windows RPC
49667/tcp open     msrpc            Microsoft Windows RPC
49668/tcp open     msrpc            Microsoft Windows RPC
49678/tcp open     msrpc            Microsoft Windows RPC
49692/tcp open     msrpc            Microsoft Windows RPC
49722/tcp open     msrpc            Microsoft Windows RPC
49723/tcp open     msrpc            Microsoft Windows RPC
```

Solution
This host should be placed behind a firewall, preferably in a DMZ network.
Additional Resources
Comments
See summary of recommendations for additional information

8.2 Medium Risk Findings

Vulnerability	IKE VPN Only Supports Insecure Hashing Algorithms (MD5 SHA1)					
Synopsis	VPN supports hashing algorithms which have been cracked					
Severity	**Medium**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 1MT	xxx.xxx.44.50	UDP 500	IKE			
Description						



Solution
Additional Resources
Comments
See summary of recommendations for additional information

Vulnerability	IKE Aggressive Mode Shared Secret Hash Leakage Weakness					
Synopsis	VPN device leaks a hashed pre-shared key					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 2MT	xxx.xxx.44.50	UDP 500	IKE			

Description

The pre-shared key for this vpn can be extracted from the device using a readily available tool

```
[illegible].50     Aggressive Mode Handshake returned
        HDR=(CKY-R=557ce3817c01ffec)
        SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x000
07080)
        KeyExchange(128 bytes)
        Nonce(16 bytes)
        ID(Type=ID_IPV4_ADDR, Value=[illegible]1.50)
        Hash(20 bytes)

IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):
e614263cb270ce85358c6d2f287243b78a64abbcaefdc27257a4089c65babf2252ca947a9a8c0e03a9ec063bd705667
2dc5ed03e038eb6edc75a017d247e41cfee54e333536888a9716331b45631974fa47284b62357a349049407fb4e6920
8ad88b46789bd1acfab6db47fa59d1a32e4c4093abbd23f29e30a18b525d20e198:a6f9cbaecc736b78daa3c857664e
a3221570a5c7110de807ef843de40c5018bfb6f41241eced49faaecd86144eb48bf62be9d6a79a1cc75075ba39c2525
e07963e645707a26796e1124e3ea63107d93f621cbaa1b1f0b3eb015364c421327db33bec6dc91fe6755f1d945bd278
354257ecfb1273fe98a99be1a0c81a2d93d0a2:557ce3817c01ffec:8cf38dab9d62b48b:0000000100000001000000
980101000403000024010100008001000580020002800300018004000280 0b0001000c0004000070800300002402010
000800100058002000180030001800400028 00b0001000c000400007080030000240301000080010001800200028003
000180040002800b0001000c000400007080000000240401000080010001800200018003000180040002800b0001000
c000400007080:011101f447292c32:0e06f43335c353432210047111ab31fa55822786:b5fd84c26b33eb70b3ec8ab
6d0a9138a:993fdc4a2f6929b4bb179ba75ae09a88b214b879
Ending ike-scan 1.9.4: 1 hosts scanned in 0.039 seconds (25.36 hosts/sec).  1 returned handshak
e; 0 returned notify
```

Solution

Additional Resources

Comments

See summary of recommendations for additional information

Vulnerability	IKE VPN SA Proposal Allows 3DES & DES					
Synopsis	3DES and DES are insecure encryption methods which should be avoided					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID: 3MT	xxx.xxx.44.50	UDP 500	IKE			

Description

The VPN devices support the use of 3DES and DES encryption standards

Solution

Configure AES-128-bit encryption as the standard

Additional Resources

Comments

See summary of recommendations for additional information

Vulnerability	ICMP is available to public NAT addresses					
Synopsis	ICMP protocol is available bi-directionally from the following public hosts					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID:4MT	xxx.xxx.6.145 xxx.xxx.6.146 xxx.xxx.6.149 xxx.xxx.6.152 xxx.xxx.6.153 xxx.xxx.6.154 xxx.xxx.37.163 xxx.xxx.44.49 xxx.xxx.44.50 xxx.xxx.44.51 xxx.xxx.44.52 xxx.xxx.44.53 xxx.xxx.145.49 xxx.xxx.145.50 xxx.xxx.145.57 xxx.xxx.145.59 xxx.xxx.145.60 xxx.xxx.145.61 xxx.xxx.145.62	all				

Description

During the reconnaissance phase of the engagement our consultants observed the ICMP protocol is available to all hosts both inside and outside the firewall. In addition to being a preferred tool for information gathering to attacks the existing of ICMP presents another serious issue that can be leveraged to maintain command and control if the system is exploited.

Through the use of ICMP tunnels an attacker could set up an ICMP tunnel which would allow RDP/SSH/Telnet packets to be encapsulated within an ICMP tunnel. Normally attackers would perform this action over the http ports using netcat but since that normally deprives the public of access to the intended service it is considered less of an ideal candidate

http://code.gerade.org/hans/

Solution

Disable ICMP accept on all perimeter devices

Additional Resources

Comments

See summary of recommendations for additional information

Vulnerability	SSL Version 2 and 3 Protocol Detection					
Synopsis	The remote service encrypts traffic using a protocol with known weaknesses					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID:5MT	xxx.xxx.37.166	443				
Description						

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Reconfigure server to only accept TLS v1.2 or above
Additional Resources
Comments
See summary of recommendations for additional information

Vulnerability	IKE Protocol Allowed from Any Source					
Synopsis	VPN connections can be initiated from any source					
Severity	Medium					
CVSS Score	0	CVE			Exploitable	
Affected Systems	IP(s)	Ports	Service	FQDN	NetBIOS Name	MAC Address
ID:6MT	xxx.xxx.44.50 xxx.xxx.6.153	UDP 500	IKE			
Description						

Client VPN connections can be initiated from any source. This, combined with the fact there is no MFA configured on remote access connections could lead to a full comprise of the network

Solution
Restrict incoming IKE connections to domestic sources and implement MFA
Additional Resources
Comments
See summary of recommendations for additional information

Vulnerability	SNMP open on public network					
Synopsis	SNMP read access using PUBLIC community string was available					
Severity	**Medium**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID:7MT	xxx.xxx.6.145	UDP 161				
Description						
During the discovery phase of the engagement our consultants were able to pull a significant amount of information about the public border router using the SNMP protocol **Note: this issue was resolved immediately by ACME IT staff**						
Solution						
Disable udp port 161 to router or craft an access list						
Additional Resources						
This finding was resolved immediately by the ACME technical team						
Comments						
See summary of recommendations for additional information						

8.3 Low Risk Findings

Vulnerability	Common Security Headers not present					
Synopsis	Common security headers which instruct browser to implement security features are not present					
Severity	**Low**					
CVSS Score	0	**CVE**			**Exploitable**	
Affected Systems	**IP(s)**	**Ports**	**Service**	**FQDN**	**NetBIOS Name**	**MAC Address**
ID: 1LO	xxx.xxx.37.166 xxx.xxx.37.165 xxx.xxx.37.170	443	SSL			

Description

Common security headers not found

- HTTP Strict Transport Security (HSTS) ...
- Content Security Policy (CSP) ...
- Cross Site Scripting Protection (X-XSS) ...
- X-Frame-Options. ...
- X-Content-Type-Options

Solution

Follow the instructions found here: https://scotthelme.co.uk/hardening-your-http-response-headers/

These instructions if followed correctly will address all security header related issues and can be tested with the following site when completed. https://securityheaders.com/

Implement a commercial or open source WAF
Open source: https://www.aqtronix.com/?PageID=114
https://geekflare.com/webknight-iis-waf/ <- instructions
Enterprise: https://www.imperva.com/products/web-application-firewall-waf/

Evaluate need for continued availability to the public: Based on the existence of an expired certificate and verbiage on the site which indicates it may be a stale web site it may be advisable to remove this server entirely

Additional Resources

Comments

See summary of recommendations for additional information

9 RISK ASSESSMENT MATRIX

Vulnerability	Likelihood	Impact	Asset	Mitigating Control	Mitigating Control Effectiveness	Residual Risk
Deep penetration into internal network through web-based vulnerabilities	High	High	Computer network,	Firewall, Inline IPS, SIEM	Sub-optimal	Medium-high
Maintain persistent control of publically accessible web after compromise	Medium	High	Computer network,	Firewall ACLs, Inline IPS	Sub-optimal	High
Take control of perimeter device outside firewall	High	Medium	Outside monitoring tools, reputation	None	Non-existent	High
DDOS Attack	Medium	High	Reputation, VPN availability for officers in field	Firewall	Sub-optimal	High
Intercept traffic through MITM-based attacks on web servers	Medium-Low	Medium	User login information	Server cryptographic engine	Ineffective	High
Deface existing pages on public webservers	Medium	Medium	Reputation	Firewall, inline IPS	Sub-optimal	Medium
Access through client VPN via compromised accounts	Medium	high	Computer network	Username and password	Sub-optimal	Medium

10 RECOMMENDATION PRIORITIZATION

1. Configure a Geo IP-based access list which will restrict access to public systems based on domestic IP address sources. This access list should be in an explicit accept default deny format. Details on domestic based IP address assignments can be found here: https://www.nirsoft.net/countryip/us.html An access list construction for ISP routers can be constructed by our Advisory & Transformation team as a separate engagement.
2. Create access lists to protect the IP-based interfaces of internet routers and devices which reside on the outside perimeter.
3. Implement a brute force protection system such as fail2bain on Ubuntu host. Instructions can be found here: https://www.linode.com/docs/guides/how-to-use-fail2ban-for-ssh-brute-force-protection/. Be sure to set Permit root login to **no** in /etc/ssh/sshd_config
4. Place outside hosts behind existing firewall.
5. Implement account lock out for all users including administrator on FTP server & switch to a more secure protocol if possible.
6. Make the necessary registry changes to the windows hosts as outlined in the findings section
7. Implement open source host based WAF as outlined in the findings section.
8. Consolidate the inline IPS, Firewall & VPN systems into a single purpose enterprise grade firewall such as a pair of FortiGate FG-200F with threat protection, fortisandbox, URL blocking, antivirus, app-id and vpn. Configure SSL interception on all inbound web connections. Configure email alerting on top 10 most critical types of attacks on the firewall.
9. Implement a radius server which ties into active directory and can integrate with Google Authenticator MFA.