Qualys. Enterprise

Scan Results

July 27, 2020

This report was generated with an evaluation version of Qualys

Report Summary

User Name:	富士通太郎
Login Name:	fujitsu
Company:	FUJITSU LIMITED
User Role:	Scanner
Address:	
City:	
Zip:	
Country:	Japan
Created:	07/27/2020 at 11:04:53 (GMT+0900)
Launch Date:	12/25/2019 at 19:47:39 (GMT+0900)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1577270859.10831
Scanner Appliances:	Demo (Scanner 11.6.51-1, Vulnerability Signatures 2.4.777-2)
Duration:	00:04:35
Title:	脆弱性診断sample
Asset Groups:	-
IPs:	10.0.0.4
Excluded IPs:	-
FQDNs:	-
Options Profile:	Initial Options

Summary of Vulnerabilities

Vulnerabilities Total	16	Security Risk (Avg)	3.0

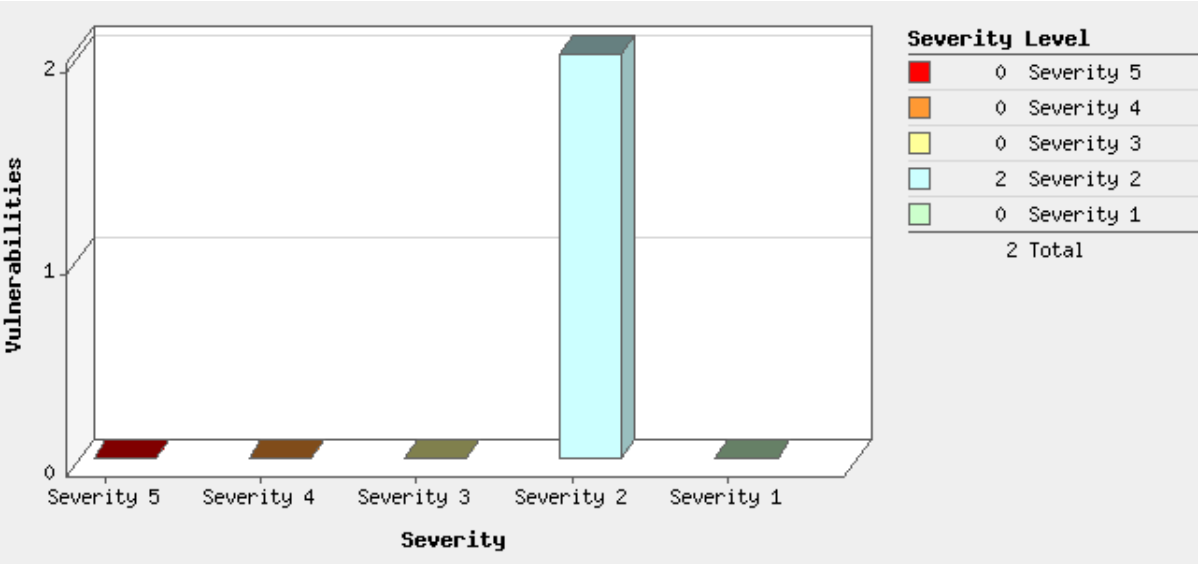
by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	1	1	2
2	2	0	2	4
1	0	0	10	10
Total	2	1	13	16

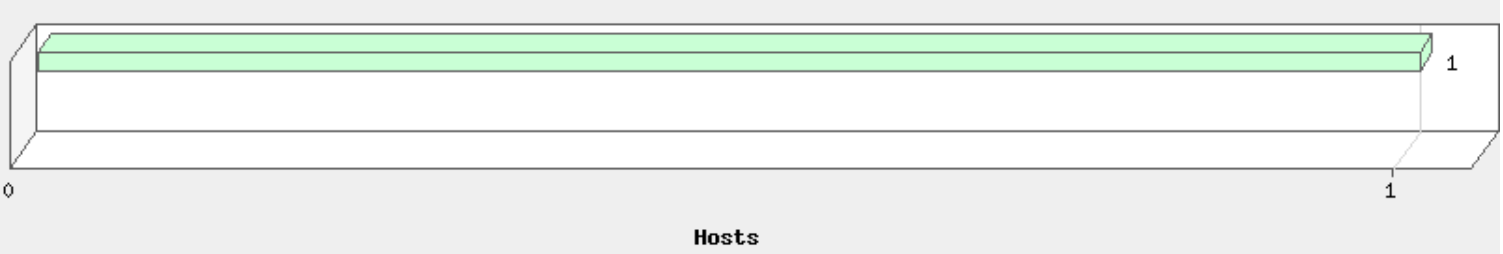
5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
TCP/IP	0	0	7	7
General remote services	1	1	3	5
RPC	1	0	1	2
Information gathering	0	0	2	2
Total	2	1	13	16

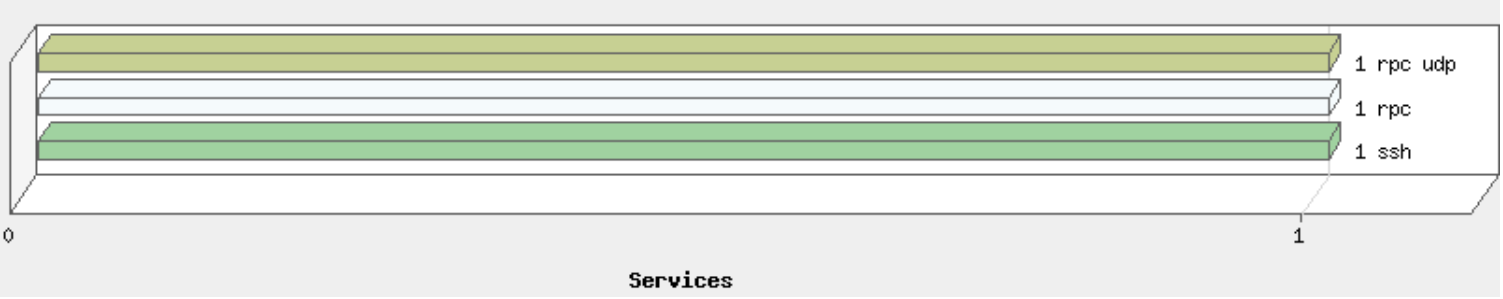
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

10.0.0.4 (-, -)

Vulnerabilities (2)

2 隠された RPC サービス (Hidden RPC Services)

QID:	11
Category:	RPC
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	01/01/1999
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
Portmapper / Rpcbind はポート番号 111 で待機し、サーバ上で起動する登録された RPC サービスの更新リスト（RPC 名、バージョン、ポート番号）を格納します。Portmapper / Rpcbind（ポートマッパ）は、クライアントが接続したい任意の RPC デーモンへのゲートウェイとして動作します。
portmapper / rpcbindが削除されたり、ファイアウォールで保護されると、標準の RPC クライアントプログラムはポートマッパリストの獲得に失敗します。しかし注意深く作られたパケットを送信すると、どの RPC プログラムがどのポートで動作しているかを特定することが可能です。この技術は、ダイレクト RPC スキャニングと呼ばれ、あるポート（TCPやUDPポート）で動作する RPC プログラムを特定する際に、portmapper / rpcbind をバイパスするために利用されます。Linux サーバでは、RPC サービスは通常、特権ポートで動作します（1024番以下）、一方 Solaris の RPC サービスでは、（32700 から始まる）短命なポートで動作します。

IMPACT:
権限のないユーザはサーバ上で動作する、RPC サービスのリストを作成することが可能です。もし権限のないユーザがホスト上で RPC サービスの脆弱性に気付けば、それを悪用することが可能です。

SOLUTION:
権限のないユーザの RPC デーモンへのアクセスの防止は、portmapper ポートのファイアウォール保護や portmapper
サービスの削除では不十分です。ホスト上で不可欠な RPC サービス以外は、全て削除してください。

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Name	Program	Version	Protocol	Port
portmap/rpcbind	100000	2-4	tcp	111
portmap/rpcbind	100000	2-4	udp	717
portmap/rpcbind	100000	2-4	udp	111

2 廃止される予定の SSH 暗号の設定 (Deprecated SSH Cryptographic Settings) port 22/tcp

QID:	38739
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/03/2019
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
SSH プロトコル（Secure Shell）はあるコンピュータから別のコンピュータへのリモートログインを安全に行うための方法です。
スキャン対象は、廃止される予定の SSH 暗号化設定を通信に使用しています。

IMPACT:

中間者攻撃を行う攻撃者は、この脆弱性を悪用して通信を記録し、セッションキーやメッセージまでも復号する可能性があります。

SOLUTION:
廃止される予定の暗号化設定は使用しないようにしてください。
SSH を設定する際には、ベストプラクティスに従ってください。
Security of Interactive and Automated Access Management Using Se
cure Shell (SSH) (https://csrc.nist.gov/publications/detail/nist
ir/7966/final)（英語）を参照してください。
現在、その設定は廃止される予定と思われます。
OFB の CFB を使用する暗号
CTR や GCM などの新しい暗号チェーンモードと比較すると脆弱であるため、非常に一般的ではなく廃止される予定です
RC4 暗号（arcfour、arcfour128、arcfour256）
RC4 暗号は、暗号化バイアスを備えていますが、現在では安全であるとは考えられていません
ブロックサイズが 64 ビットの暗号（DES、3DES、Blowfish、IDEA、CAST）
ブロックサイズが 64 ビットの暗号は誕生日攻撃に対して脆弱です（Sweet32）
DH グループ 1（diffie-hellman-group1-sha1、gss-group1-sha1-*）を使用する鍵交換
のアルゴリズム
DH グループ 1 は 1024 ビット長の鍵を使用しますが、それは短すぎて Logjam 型の攻撃に対して脆弱であると考えら
れています
鍵交換アルゴリズム rsa1024sha1 ”
RSA 鍵のサイズが短いために非常に一般的ではなく、廃止される予定です
MAC アルゴリズム umac-32 ”
MAC 長が非常に短いために非常に一般的ではなく、廃止される予定です
暗号化 なし ”
これは SSHv1 でのみ利用可能です

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Type	Name
key exchange	diffie-hellman-group1-sha1
cipher	blowfish-cbc
cipher	cast128-cbc
cipher	3des-cbc

Potential Vulnerabilities (1)

3 OpenSSH にユーザ名列挙の脆弱性 (OpenSSH Username Enumeration Vulnerability)

QID:	38726
Category:	General remote services
CVE ID:	CVE-2018-15473
Vendor Reference:	OpenBSDH OpenSSH
Bugtraq ID:	105140
Service Modified:	07/23/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes

THREAT:
OpenSSH（OpenBSD Secure Shell）は、SSH プロトコルを使用して、暗号化された通信セッションをコンピュ
ータネットワーク上で提供するコンピュータプログラムのセットです。
OpenSSH にユーザ名列挙の脆弱性があるため、リモートの攻撃者はこれを利用して、標的のシステム上の有効なユーザを列挙すること
ができます。ユーザは悪意のあるパケットを送信することで、ユーザの列挙を試行することができます。この脆弱性により、ユーザ名が存在し
ていなかった場合、サーバは攻撃者に対して SSH2_MSG_USERAUTH_FAILURE メッセージを送信します。ユーザ名が
存在している場合、サーバは fatal() を呼び出して接続を閉じる前に SSH2_MSG_SERVICE_ACCEPT を送信
します。

影響を受けるバージョン:
OpenSSH 7.7 以下
QID の検出ロジック:
認証済みの場合：ssh -V コマンドを実行することにより、脆弱性のある OpenSSH バージョンが検出されます。
未認証の場合：表示されるバナーから、脆弱性のある OpenSSH バージョンが検出されます。

IMPACT:
脆弱性の利用に成功すると、攻撃者は標的システム上のユーザ名を列挙することができます。

SOLUTION:
この脆弱性を修正するために、OpenSSH 7.8 (https://www.openbsd.org/) またはそれ以降（英語）
にアップグレードしてください。
Patch:
Following are links for downloading patches to fix the vulnerabilities:
OpenSSH 7.8 or later: （英語） (https://www.openbsd.org/)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
Metasploit

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dreambox_openpli_shell
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/gather/credentials/gpp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/ssh/ssh_enumusers
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/multi/http/apache_roller_ognl_injection
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/samba/chain_reply
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/post/windows/manage/ie_proxypac
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/auxiliary/scanner/http/ektron_cms400net
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/dlink_dspw215_info_cgi_bof
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

Reference: CVE-2018-15473
Description: SSH Username Enumeration - Metasploit Ref : /modules/exploit/linux/http/docker_daemon_tcp
Link: https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/ssh/ssh_enumusers.rb

The Exploit-DB

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration - The Exploit-DB Ref : 45233
Link: http://www.exploit-db.com/exploits/45233

Reference: CVE-2018-15473
Description: OpenSSH < 7.7 - User Enumeration (2) - The Exploit-DB Ref : 45939

Link: http://www.exploit-db.com/exploits/45939

Reference: CVE-2018-15473
Description: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) - The Exploit-DB Ref : 45210
Link: http://www.exploit-db.com/exploits/45210

Qualys
Reference: CVE-0000-0000
Description: OpenSSH Username Enumeration
Link: http://seclists.org/oss-sec/2018/q3/125

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable SSH-2.0-OpenSSH_7.4 detected on port 22 over TCP.

Information Gathered (13)

3 リモートアクセスまたは管理サービスの検出 (Remote Access or Management Service Detected)

QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
リモートアクセスまたはリモート管理サービスが検出されました。悪意を持つユーザがこうしたサービスにアクセス可能である場合、新たなタイプの攻撃を実行するために使用される可能性があります。悪意のあるユーザがクレデンシャルに対する総当り攻撃を実行しようとしたり、新たな攻撃を細工する際にそれを可能にする、サービスに関する詳細情報を収集することができます。
Results セクションには、対象上に見つかった、リモートアクセスサービスに関する情報が含まれています。
Telnet、Rlogin、SSH、Windows リモートデスクトップ、pcAnywhere、Citrix Managemen
t Console、Remote Admin (RAdmin)、VNC、OPENVPN、および ISAKMP などのサービスはチェックされます。

IMPACT:
結果は攻撃の種類によって変ります。

SOLUTION:
リモートアクセスまたはリモート管理サービスは、システム管理者または特定の目的を帯びたシステムユーザのみが取り扱うようにします。

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: SSH on TCP port 22.

2 TCP TimeStamp オプションを基に推測したホストのアップタイム (Host Uptime Guess Based on TCP TimeStamp Option)

QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/30/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ホスト上の TCP/IP スタックは、TCP TimeStamp（kind 8）オプションをサポートしています。通常、使用されるタイムスタンプは、さまざまなユニット（例：1/100 秒、1/10 秒など）におけるホストの（前回リブートしてからの）アップタイムです。これに基づいて、ホストのアップタイムを知ることができます。結果は以下の Result セクションにあります。
OS の中には、タイムスタンプに 0 以外の初期値（おそらくランダム値）を使用するものがあります（例： MacOS、OpenBSD）。これらの OS に関しては、入手されるアップタイムはホストの実際のアップタイムを反映していません； 必ず前者（入手される方）のアップタイムが後者（実際のアップタイム）よりも大きな値となります。

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Based on TCP timestamps obtained via port 111, the host's uptime is 0 days, 0 hours, and 8 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

2 公開 RPC サービスのリスト (Open RPC Services List) port 111/tcp

QID:	9
Category:	RPC
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/25/2019
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
アクセス可能なすべての RPC サービスのマップ作成に、ポートスキャナが使用されました。

IMPACT:
これに続けて、権限のないユーザが各公開サービスに関連する脆弱性を試す可能性があります。

SOLUTION:

リスト上にある、不明または未使用のサービスをすべて停止してください。単にファイアウォールでポート 111 をフィルタリングするだけでは、すべての RPC サービスを削除することはできません。ポート 111（“ portmap ”サービス）は、どのポートが RPC サービスをリッスンしているかを示しているだけであるためです。そのため、これらのサービスへのアクセスを遮断することはできません。各 RPC サービスは UDP または TCP のエフェメラルポートをリッスンするので、サーバレベルで RPC サービスを無効にしてください。

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

program	version	protocol	port	name
100000	4	tcp	111	rpcbind
100000	3	tcp	111	rpcbind
100000	2	tcp	111	rpcbind
100000	4	udp	111	rpcbind
100000	3	udp	111	rpcbind
100000	2	udp	111	rpcbind

1 DNS ホスト名 (DNS Host Name)

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/05/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
DNS サーバから、このコンピュータのホスト名を入手できる場合、入手したホスト名が RESULT セクションに表示されます。

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
10.0.0.4	No registered hostname

1 ホストのスキャン時間 (Host Scan Time)

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/19/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ホストのスキャン時間（Host Scan Time）は、スキャンエンジンが 1 つの対象ホストの脆弱性を評価するのにかかる時間です。このホストのスキャン時間は、以下の「Result」項の「Host Scan Time」に報告されています。
「Host Scan Time」は、スキャン結果レポート内の「Report Summary」項に表示される「Duration」の時間との直接的な相関関係はありません。「Duration」は、サービスがスキャンタスクを実行するのにかかる時間です。「Duration」には、サービスがすべてのホストをスキャンするのにかかる時間が表示され、スキャンが並行して実行されている場合があります。また、Scanner Appliance がスキャンタスクを実行して結果をセキュアオペレーションセンターに送信するまでの時間も含まれています。さらに、スキャンタスクが複数のスキャナに分散されている場合は、すべてのスキャナで並行して実行されているホストのスキャンにかかる時間が「Duration」に表示されます。
Qualys Windows エージェントを実行するホストでは、この QID により、エージェントが最新の評価スキャンに使用されるホストメタデータを収集するのにかかる時間が報告されます。

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 260 seconds

Start time: Wed, Dec 25 2019, 10:50:26 GMT

End time: Wed, Dec 25 2019, 10:54:46 GMT

1 公開 UDP サービスの一覧 (Open UDP Services List)

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ポートスキャナを使用して、このホスト上にあるインターネットからアクセス可能なすべての UDP サービスのマップを作成しました。
ホストがファイアウォールの背後にあると、ファイアウォールでフィルタあるいは遮断されているが、実際には対象ホスト上でオープンでない

ポートがいくつかリストの中に含まれることがまれにあります。これ（UDP オープンポートの誤検出）は、ファイアウォールが ICMP Port Unreachable パケットを持つ（すべてではありませんが）ほとんどのポートに対する UDP パケットを拒否するよう設定されているときに起こる可能性があります。また、ファイアウォールが UDP パケットに（すべてではありませんが）ほとんどのポートの通過を許可している場合や、わずかなポートのみに対する filter/block/drop UDP パケットを許可している場合にも、これが起こる可能性があります。どちらのケースも一般的ではありません。

IMPACT:
権限のないユーザがこの情報を利用して、各公開サービス内の脆弱性を試すことができます。

SOLUTION:
リスト上にある、不明または未使用のサービスをすべて停止してください。もしどのサービスがどのプロセスやプログラムによって提供されているか不明な場合は、システム管理者に連絡して下さい。またこの種のポートスキャナの検知に利用可能な、商用あるいはオープンソースの侵入検知システムの詳細については、CERT の Web サイト (http://www.cert.org)（英語）をご覧ください。

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
68	bootpc	Bootstrap Protocol Client	unknown
111	sunrpc	SUN Remote Procedure Call	rpc udp

1 公開 TCP サービスの一覧 (Open TCP Services List)

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2009
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ポートスキャナにより、権限のないユーザが適切なツールを使用して、このホスト上のインターネットからアクセス可能なすべてのサービスのマップを作成することができます。サーバが実際の接続ログを記録しないように、このテストは ”ステルス ”ポートスキャナを使って実行されました。
Results セクションには、ポート番号（Port）、ポートでリッスンするデフォルトサービス（IANA Assigned Ports/Services）、サービスの説明（Description）、サービス検出機能を使用してスキャナが検出したサービス（Service Detected）が表示されます。

IMPACT:
権限のないユーザがこの情報を利用して、各公開サービス内の脆弱性を試すことができます。

SOLUTION:
リスト上にある、不明または未使用のサービスをすべて停止してください。もしどのサービスがどのプロセスやプログラムによって提供されているか不明な場合は、システム管理者に連絡して下さい。またこの種のポートスキャナの検知に利用可能な、商用あるいはオープンソースの侵入検知システムの詳細については、CERT の Web サイト (http://www.cert.org)（英語）をご覧ください。

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
111	sunrpc	SUN Remote Procedure Call	rpc	

1 ICMP からの返信を受信 (ICMP Replies Received)

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/17/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP（Internet Control and Error Message Protocol）は、IP パケット内でカプセル
化されたプロトコルです。ICMP の主な用途は、各ゲートウェイに対して、他のゲートウェイあるいはホストとの相互接続性やアクセス性
を通知するプロトコル層を提供することです。
ホストが ICMP 返信を送信するよう、以下の型のパケットを送信しました:
Echo Request (Echo Reply をトリガするため)
Timestamp Request (Timestamp Reply をトリガするため)
Address Mask Request (Address Mask Reply をトリガするため)
UDP Packet (Port Unreachable Reply をトリガするため)
IP Packet with Protocol >= 250 (Protocol Unreachable Reply をト
リガするため)
“ Result ”セクションに表示されている一覧が、受信した ICMP 返信です。

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Unreachable (type=3 code=3)	UDP Port 31335	Port Unreachable
Time Stamp (type=14 code=0)	Time Stamp Request	10:50:27 GMT
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 10276	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 555	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 51109	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 26409	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 9875	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 48092	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1011	Port Unreachable

Unreachable (type=3 code=3)	UDP Port 15253	Port Unreachable

1 TCP 初期シーケンス番号のランダム性の度合い (Degree of Randomness of TCP Initial Sequence Numbers)

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/20/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ホストからの SYNACK 応答で得た TCP
初期シーケンス番号（ISN）を、どの程度ランダムであるか分析しました。後続 ISN
と平均からの標準偏差の間における、平均的な変化が RESULT
セクションに表示されています。また、添付されているのはホストが使用する TCP ISN
作成スキームを利用する際の難易度です。

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Average change between subsequent TCP initial sequence numbers is 1160069590 with a standard deviation of 643614797. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5138 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

1 IP ヘッダの ID 値のランダム性 (IP ID Values Randomness)

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/28/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ホストからの IP パケット内に含まれている IP ヘッダの識別（ID）フィールド値を分析し、どの程度ランダムであるのかを判定しました。ネットワークバイトオーダーとホストバイトオーダーどちらかのうち、連続した 2 つの ID 値の変化が小さい方を、探査の送信にかかった時間と共に、RESULT セクションに表示しています。増分値が使用される際（多くの OS の TCP/IP 実装によくあるケースです）には、これらの変化は、このテストが実施された当時のホストのネットワーク負荷を表しています。
信頼性の理由により、開かれた TCP ポートからのネットワークトラフィックのみを分析している点を留意ください。

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 111: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 23 milli seconds

1 利用できないホスト名 (Host Name Not Available)

QID:	82056
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/08/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
このホストの、完全修飾ドメイン名（FQDN）あるいは Netbios 名を取得しようとしましたが、取得に失敗しました。

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

No results available

1 SSH デーモン情報の検索 (SSH daemon information retrieving) port 22/tcp

QID:	38047
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/05/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSH は、完全にパッチが施され、正しく設定され、FIPS で承認されたアルゴリズムを使用するなら、安全なプロトコルです。
Red Hat ES 4 の場合:-
サポートされている SSH1　あり
SSH1 についてサポートされている認証方式 RSA,password
SSH1 についてサポートされている暗号　3des,blowfish
サポートされている SSH2　あり
SSH2 についてサポートされている鍵交換アルゴリズム diffie-hellman-group-exchange-sha1,d
iffie-hellman-group14-sha1,diffie-hellman-group1-sha1
SSH2 についてサポートされている復号　aes128-cbc,3des-cbc,blowfish-cbc,cast128-c
bc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes
128-ctr,aes192-ctr,aes256-ctr
SSH2 についてサポートされている暗号化　aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,ae
s128-ctr,aes192-ctr,aes256-ctr
SSH2 についてサポートされている複号化 mac　hmac-md5,hmac-sha1,hmac-ripemd160,hma
c-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
SSH2 についてサポートされている暗号化 mac　hmac-md5,hmac-sha1,hmac-ripemd160,hma
c-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
SSH2 についてサポートされている認証方式 publickey,gssapi-with-mic,password

IMPACT:
悪用に成功すると、攻撃者は SSH サーバ上で任意のコマンドを実行できたり、あるいは暗号化した SSH
チャンネルを任意のデータで破壊できるようになります。

SOLUTION:
SSH バージョン 2 が SSH バージョン 1 に優先します。

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
Supported host key algorithms for SSH2	ssh-rsa, rsa-sha2-512, rsa-sha2-256, ecdsa-sha2-nistp256, ssh-ed25519
Supported decryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-cbc, aes192-cbc, aes256-cbc, blowfish-cbc, cast128-cbc, 3des-cbc
Supported encryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-cbc, aes192-cbc, aes256-cbc, blowfish-cbc, cast128-cbc, 3des-cbc
Supported decryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported encryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey, gssapi-keyex, gssapi-with-mic, password, keyboard-interactive

1　SSH バナー (SSH Banner)　port 22/tcp

QID:　38050
Category:　General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/05/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_7.4

Appendix

Hosts Scanned (IP)

10.0.0.4

Target distribution across scanner appliances

: 10.0.0.4

Options Profile

Initial Options

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Vulnerability Detection:	Complete
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Disabled
Unix/Cisco:	Disabled
Oracle:	Disabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Jboss Server:	Disabled
Oracle WebLogic Server:	Disabled
MariaDB:	Disabled
InformixDB:	Disabled
MS Exchange Server:	Disabled
Oracle HTTP Server:	Disabled
MS SharePoint:	Disabled
Sybase:	Disabled
Overall Performance:	Normal
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	15
Scanner Appliances:	30

Processes to Run in Parallel:	
Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore firewall-generated TCP RST packets:	Off
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	Off
Do not send TCP ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Severity	Level	Description
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

This report was generated with an evaluation version of Qualys