TRIPWIRE® IP360

TECHNICAL ANALYSIS

Thu July 20, 2017

Networks

2017_yamada-lab

Report Summary 1
Technical Analysis Summary . . . 1

Hosts 3
Hosts . . . 3
133.9.193.169 . . . 4
133.9.193.144 . . . 7

Vulnerabilities 11
Vulnerabilities . . . 11
SSH Insecure HMAC Algorithms Enabled . . . 12
SSH RC4 Cipher Enabled . . . 13
SMTP Available . . . 14
SSH Protocol Available . . . 15
DNS Available . . . 16
HTTP Available . . . 17
E-Mail Services Available . . . 18
Untrusted SSL/TLS Certificate . . . 19
NO SSH AUTHENTICATION ATTEMPTED (no credentials configured) . . . 21
SSL Certificate Information . . . 23
SSH CBC Mode Ciphers Enabled . . . 24
SSL Server Supports CBC Ciphers for TLSv1 . . . 25
SSL Certificate Key Length < 4096 bits . . . 27
SSL Certificate Key Length <= 2048 bits . . . 29
SSL Certificate Key Length <= 4096 bits . . . 31
TLSv1 Enabled . . . 33
TLSv1.1 Enabled . . . 34
RFC7525 - Insecure TLS Protocol Version Exposure (Strict TLS) . . . 35
RFC7525 - TLS Transition Exposure . . . 36
RFC7525 First Cipher Preference Exposure . . . 37
RFC7525 - Insecure TLS Protocol Version Exposure (POP3) . . . 38
BIND Version . . . 39
TLS RFC7627 Extended Master Secret Computation Not Supported . . . 41
POP3 Available . . . 43

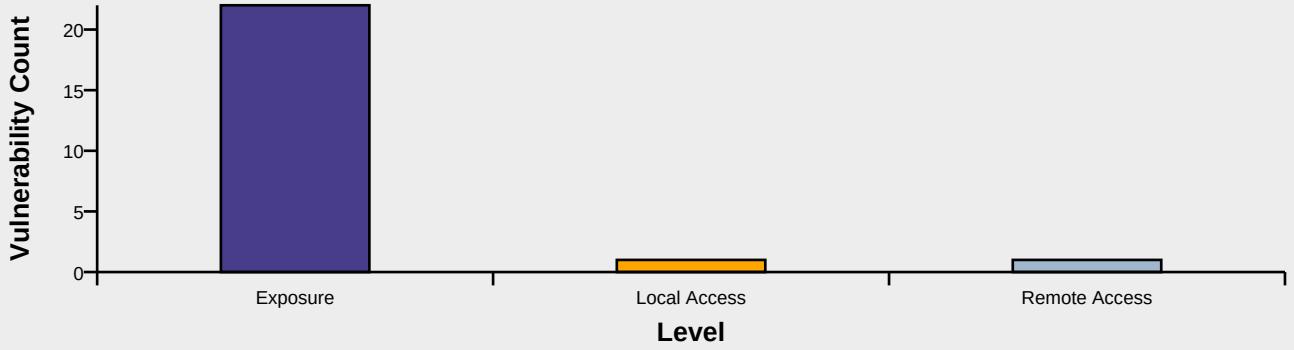
Applications 44
Applications . . . 44

Audits 45
Audits . . . 45

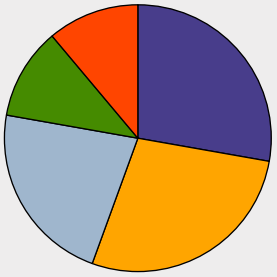
Report Summary

Start Date	07/15/2017 15:19:35	End Date	07/20/2017 15:19:35
Networks/Network Groups	2017_yamada-lab	Filters	None
Hosts	2	Asset Value	0
Average Host Score	89	Vulnerabilities	24
Applications/Services	17		

Vulnerability Level Distribution

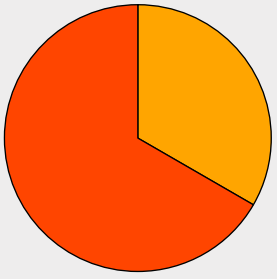


Service Distribution



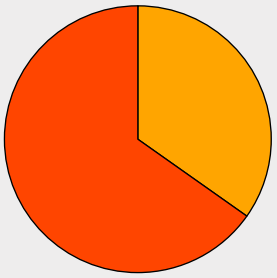
- Other (28%)
- HTTPS (28%)
- POP3 (22%)
- HTTP (11%)
- SSH (11%)

OS Distribution by OS Group



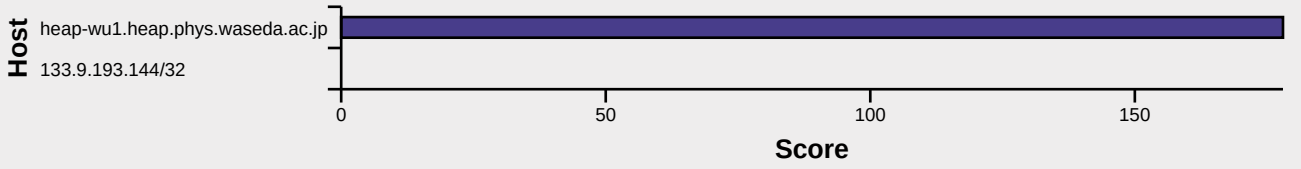
- Tripwire: Cisco (0%)
- Tripwire: Linux (33%)
- Tripwire: Network Infrastructure (0%)
- Tripwire: Sun Microsystems (0%)
- Tripwire: Unix Variant (67%)
- Tripwire: Windows (0%)

Vuln Distribution by OS Group

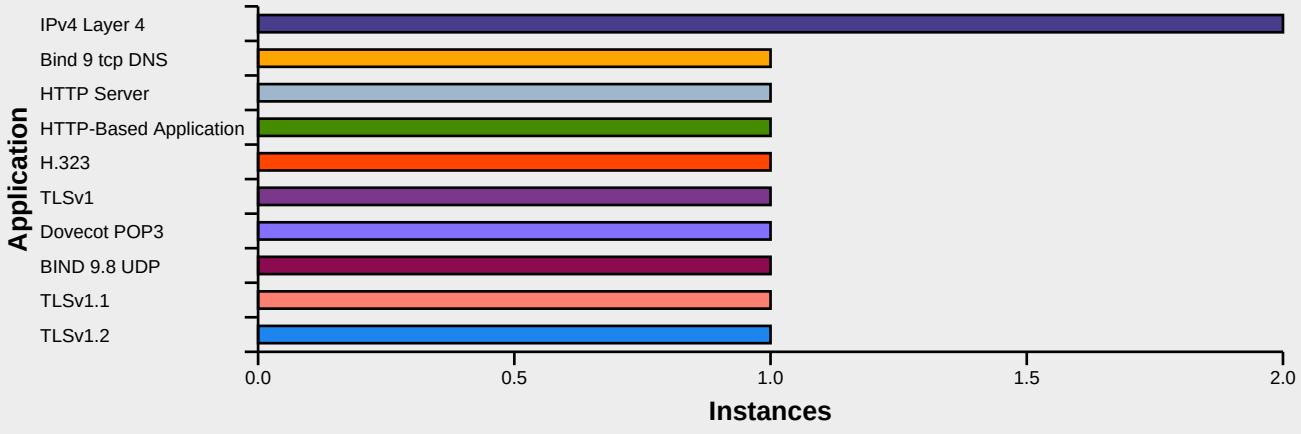


- Tripwire: Cisco (0%)
- Tripwire: Linux (35%)
- Tripwire: Network Infrastructure (0%)
- Tripwire: Sun Microsystems (0%)
- Tripwire: Unix Variant (65%)
- Tripwire: Windows (0%)

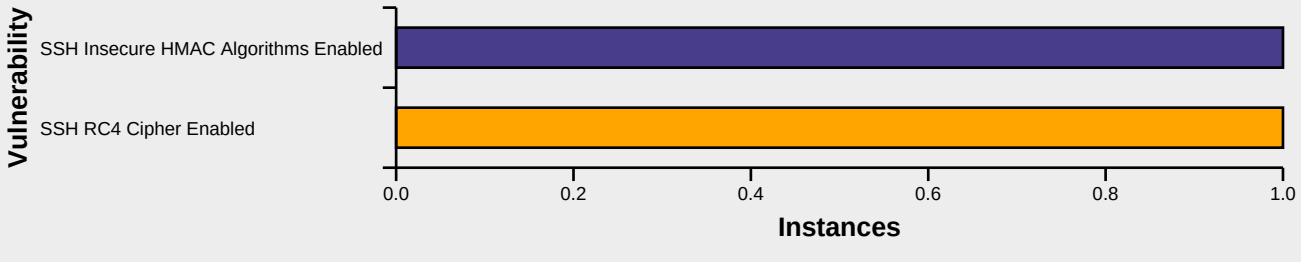
Top 10 Most Vulnerable Hosts



Top 10 Applications by Instance



Top 10 Vulnerabilities by Instance



Hosts

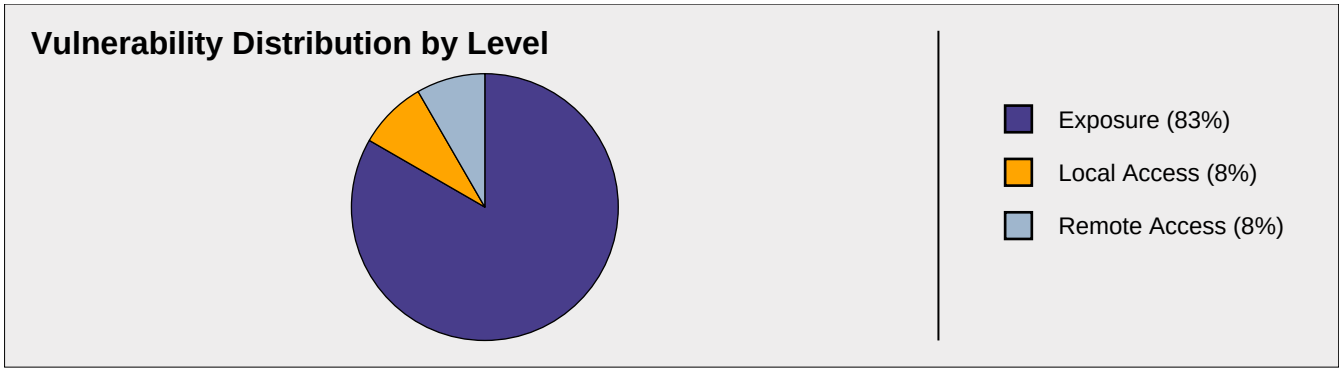
Hostname	IP Address	OS	Owner	Asset Value	Score
heap-wu1.heap.phys.waseda.	133.9.193.169	Unix Variant	None	0	178
Name not in DNS	133.9.193.144	Linux	None	0	0

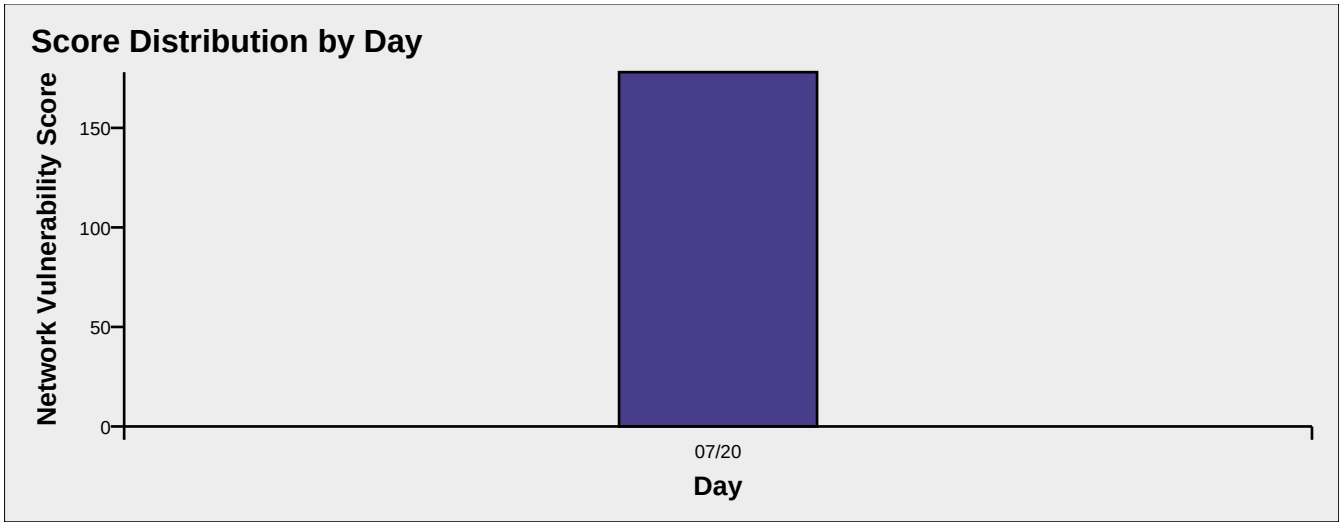
Host Summary

Hostname	heap-wu1.heap.phys.waseda.ac.jp	IP Address	133.9.193.169
Score	178	Asset Value	0
OS Name	Unix Variant	Owner	None
NetBIOS Name		Mac Address (NetBIOS)	
Domain/Workgroup			

Operating System

OS Name
Unix Variant





Vulnerabilities

Vulnerability	CVE	# of Ports	Score

continued on next page

Vulnerability	CVE	# of Ports	Score
SSH Insecure HMAC Algorithms Enabled		1	175
SSH RC4 Cipher Enabled	CVE-2013-2566	1	3
SMTP Available		1	0
SSH Protocol Available		1	0
DNS Available		1	0
E-Mail Services Available		2	0
NO SSH AUTHENTICATION ATTEMPTED (no credentials configured)		1	0
SSH CBC Mode Ciphers Enabled		1	0
RFC7525 - TLS Transition Exposure		1	0
BIND Version		1	0
RFC7525 - Insecure TLS Protocol Version Exposure (POP3)		1	0
POP3 Available		1	0

Applications

Service	Application	Port
DNS TCP	Bind 9 tcp DNS	53
DNS UDP	BIND 9.8 UDP	53
IPv4 Layer 4		0
POP3	Dovecot POP3	110
POP3	TLS Capable POP3 Server (TLSv1)	110
POP3	TLS Capable POP3 Server (TLSv1.1)	110
POP3	TLS Capable POP3 Server (TLSv1.2)	110
SMTP	Postfix 2.x	25
SSH	OpenSSH 6.4	22

Configuration Checks

Configuration Check	Discovery Method	Value
Nmap OS String	TCP	
Nmap Status	NMAP	Global: Nmap Not Configured
SSH Compression Algorithms	TCP	none, zlib@openssh.com
SSH Encryption Algorithms	TCP	aes128-ctr, aes192-ctr, aes256-ctr, arcfour256, arcfour128, aes128-gcm@openssh.com, aes256-gcm@openssh.com, aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, aes192-cbc, aes256-cbc, arcfour, rijndael-cbc@lysator.liu.se, hmac-md5-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-ripemd160-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-md5, hmac-sha1, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-ripemd160, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96

continued on next page

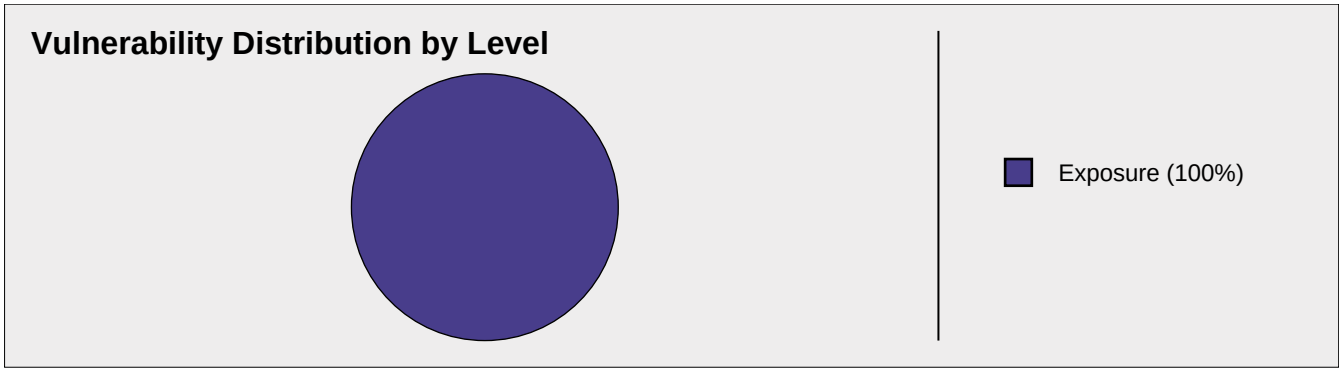
Configuration Check	Discovery Method	Value
SSH Host Key Algorithms	TCP	ssh-rsa, ssh-dss, ecdsa-sha2-nistp256
SSH Key Exchange Algorithms	TCP	ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
WDRT Authentication Success	TCP	False
WDRT_Access	TCP	WDRT_SMB_AUTH_SUCCESS : False, WDRT_SMB_REGISTRY_ACCESS : False, WDRT_SMB_FILE_ACCESS : False, WDRT_RPC_AUTH_SUCCESS : False, WDRT_WMI_AUTH_SUCCESS : False, WDRT_HOST_IS_64BIT : False,

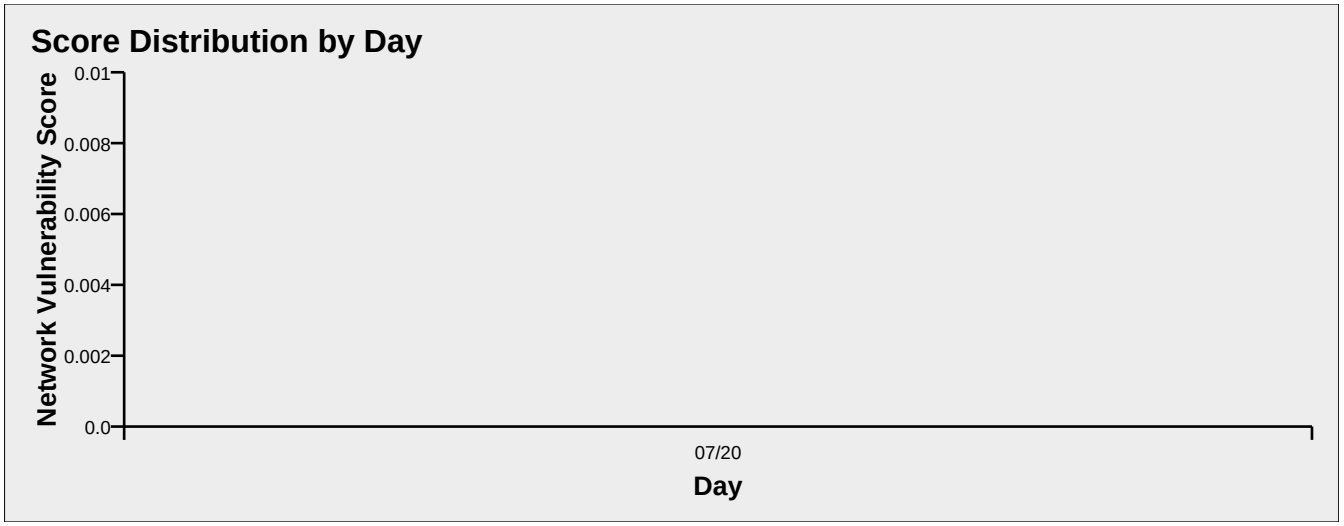
Host Summary

Hostname	Name not in DNS	IP Address	133.9.193.144
Score	0	Asset Value	0
OS Name	Linux	Owner	None
NetBIOS Name		Mac Address (NetBIOS)	
Domain/Workgroup			

Operating System

OS Name
Linux





Vulnerabilities

Vulnerability	CVE	# of Ports	Score
SSH Protocol Available		1	0

continued on next page

Vulnerability	CVE	# of Ports	Score
HTTP Available		2	0
Untrusted SSL/TLS Certificate		1	0
NO SSH AUTHENTICATION ATTEMPTED (no credentials configured)		1	0
SSL Certificate Information		1	0
SSH CBC Mode Ciphers Enabled		1	0
SSL Server Supports CBC Ciphers for TLSv1		1	0
SSL Certificate Key Length < 4096 bits		1	0
SSL Certificate Key Length <= 2048 bits		1	0
SSL Certificate Key Length <= 4096 bits		1	0
TLSv1 Enabled		1	0
TLSv1.1 Enabled		1	0
RFC7525 - Insecure TLS Protocol Version Exposure (Strict TLS)		1	0
RFC7525 First Cipher Preference Exposure		1	0
TLS RFC7627 Extended Master Secret Computation Not Supported		1	0

Applications

Service	Application	Port
H.323		1720
HTTP	HTTP Server	80
HTTP	HTTP-Based Application	80
HTTPS	HTTP Server	443
HTTPS	HTTP-Based Application	443
HTTPS	TLSv1	443
HTTPS	TLSv1.1	443
HTTPS	TLSv1.2	443
IPv4 Layer 4		0
Open TCP Port	N/A	5001
SSH	OpenSSH 6.7	22

Configuration Checks

Configuration Check	Discovery Method	Value
HTTP Server Banners	tcp	Port 80: lighttpd, Port 443: lighttpd
Nmap OS String	TCP	Linux 2.6.36 - 2.6.37
Nmap Status	NMAP	Global: Nmap Not Configured
SSH Compression Algorithms	TCP	none, zlib@openssh.com
SSH Encryption Algorithms	TCP	aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com, aes128-cbc, 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

continued on next page

Configuration Check	Discovery Method	Value
SSH Host Key Algorithms	TCP	ssh-dss, ssh-rsa
SSH Key Exchange Algorithms	TCP	curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
SSL Certificate Extended Key Usage	SSL	TCP(443): serverAuth clientAuth
SSL Certificate Issuer	SSL	TCP(443): commonName=Polycom Equipment Issuing CA 2
SSL Certificate Key Usage	SSL	TCP(443): keyEncipherment dataEncipherment digitalSignature
SSL Certificate MD5 Thumbprint	SSL	TCP(443): 68:B0:CF:BA:85:39:D1:28:46:9E:79:09:64:EA:61:FD
SSL Certificate Public Key Size	SSL	TCP(443): 2048 bits
SSL Certificate SHA1 Thumbprint	SSL	TCP(443): 07:1B:07:38:7B:10:D9:52:29:FA:01:06:0D:4C:00:50:82:CD:4F:29
SSL Certificate Serial Number	SSL	TCP(443): 6D:58:47:63:00:00:00:80:52:AA
SSL Certificate Signature Algorithm	SSL	TCP(443): sha256WithRSAEncryption
SSL Certificate Subject	SSL	TCP(443): commonName=00E0DB44B9A4\, organizationName=Polycom Inc.
SSL Certificate Valid From	SSL	TCP(443): Tue Oct 6 05:07:51 2015 UTC
SSL Certificate Valid To	SSL	TCP(443): Sun Oct 6 05:17:51 2030 UTC
TLSv1 CBC Ciphers	SSL	The following CBC ciphers are supported on TCP(443): TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (256-bit)\, TLS_RSA_WITH_3DES_EDE_CBC_SHA (192-bit)\, TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (192-bit)\, TLS_RSA_WITH_AES_128_CBC_SHA (128-bit)\, TLS_DHE_RSA_WITH_AES_128_CBC_SHA (128-bit)\, TLS_RSA_WITH_AES_256_CBC_SHA (256-bit)\, TLS_DHE_RSA_WITH_AES_256_CBC_SHA (256-bit)\, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (168-bit)
TLSv1.2 Strong Ciphers	SSL	The following strong TLSv1.2 ciphers are supported on TCP(443): TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (256-bit)\, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (256-bit)\, TLS_RSA_WITH_AES_256_GCM_SHA384 (256-bit)\, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (128-bit)\, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (128-bit)\, TLS_RSA_WITH_AES_128_GCM_SHA256 (128-bit)
WDRT Authentication Success	TCP	False
WDRT_Access	TCP	WDRT_SMB_AUTH_SUCCESS : False, WDRT_SMB_REGISTRY_ACCESS : False, WDRT_SMB_FILE_ACCESS : False, WDRT_RPC_AUTH_SUCCESS : False, WDRT_WMI_AUTH_SUCCESS : False, WDRT_HOST_IS_64BIT : False,

continued on next page

Configuration Check	Discovery Method	Value

Vulnerabilities

Vulnerability	CVE	Hosts	Score
SSH Insecure HMAC Algorithms Enabled		1	175
SSH RC4 Cipher Enabled	CVE-2013-2566	1	3
SMTP Available		1	0
SSH Protocol Available		2	0
DNS Available		1	0
HTTP Available		1	0
E-Mail Services Available		1	0
Untrusted SSL/TLS Certificate		1	0
NO SSH AUTHENTICATION ATTEMPTED (no credentials configured)		2	0
SSL Certificate Information		1	0
SSH CBC Mode Ciphers Enabled		2	0
SSL Server Supports CBC Ciphers for TLSv1		1	0
SSL Certificate Key Length < 4096 bits		1	0
SSL Certificate Key Length <= 2048 bits		1	0
SSL Certificate Key Length <= 4096 bits		1	0
TLSv1 Enabled		1	0
TLSv1.1 Enabled		1	0
RFC7525 - Insecure TLS Protocol Version Exposure (Strict TLS)		1	0
RFC7525 - TLS Transition Exposure		1	0
RFC7525 First Cipher Preference Exposure		1	0
RFC7525 - Insecure TLS Protocol Version Exposure (POP3)		1	0
BIND Version		1	0
TLS RFC7627 Extended Master Secret Computation Not Supported		1	0
POP3 Available		1	0

Vulnerability

Vulnerability Name	SSH Insecure HMAC Algorithms Enabled	Score	175
Published	2010-01-01	Strategy	Data-Driven Attack
	nCircle: 78685	CVSS v2	4.0
CVSS v3	5.4		

Description

DESCRIPTION
Insecure HMAC Algorithms are enabled
SOLUTION
Disable any 96-bit HMAC Algorithms.
Disable any MD5-based HMAC Algorithms.

Affected Applications

Application Name
SSH

Advisory Publisher Entries

Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE { from aspl_env import getContextVariable
try:  test_data = getContextVariable('ssh_server_to_clie
nt_mac') + getContextVariable('ssh_client_to_server_mac') except KeyError:  rule.STOP(False)
for item in t
est_data:  if item.endswith('-96'):  rule.STOP(True) elif 'md5' in item:  rule.STOP(True)
rule.STOP(False) }
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	SSH RC4 Cipher Enabled	Score	3
Published	2006-01-01 nCircle: 78683	Strategy	Data-Driven Attack
		CVSS v2	4.3
CVSS v3	5.4		

Description

DESCRIPTION
The arcfour cipher is considered to be flawed.
SOLUTION
Disable the arcfour cipher.

Affected Applications

Application Name
SSH

Advisory Publisher Entries

BugTraq: 58796	http://www.securityfocus.com/bid/58796
CVE:CVE-2013-2566	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566
CWE: 310	http://cwe.mitre.org/data/definitions/310.html
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE { from aspl_env import getContextVariable
try:  test_data = getContextVariable('ssh_client_to_ser
ver_ciphers') + getContextVariable('ssh_server_to_client_ciphers') except KeyError:  rule.STOP(False)
if '
arcfour' in test_data:  rule.STOP(True)
rule.STOP(False) }
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	SMTP Available	Score	0
Published	nCircle: 1064	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

SMTPは、トランスポートサービス環境間でメールを送信するためのプロトコルです。送信側プロセスと受信側プロセス間のTCP接続は、デフォルトのポート25による伝送チャネルを提供します。SMTPは、送信サブシステムに依存しないため、信頼性のある、順序づけられたデータストリームチャネルのみを必要とします。SMTPのプロトコルは、RFC-821に定義されています。

解決策: SMTPデーモンがサーバ運用に必要なければ、使用不可に設定してください。不必要なサービスを排除することで、攻撃ポイントとなりうる要素を除去し、ネットワークに対するリスクを軽減できます。SMTPが必要な場合は、暗号化をお勧めします。

Affected Applications

Application Name
SMTP

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	SSH Protocol Available	Score	0
Published		Strategy	Network Reconnaissance
	nCircle: 1191	CVSS v2	0.0
CVSS v3	0.0		

Description

Secure Shell (SSH)がサーバー上で検知されました。技術的な詳細説明:SSH はサーバー上で使用可能であり、リモートユーザーがそのバージョンを確認する可能性があります。これは必ずしも深刻な脆弱性とはいえませんが、アクセス制御リストや他のファイアウォール技術は任意のポートへの不当なアクセス、又はバナー情報を表示するアプリケーションを阻止するために使用する必要があるということに注意すべきです。遠隔地の攻撃者は、情報収集を実行する目的で、システムのタイプとアプリケーションのバージョンを判断するためにバナー情報を使用することが可能です。解決策:SSH に対する外部アクセスが必要ない場合は、ファイアウォールとルータ上のパケットフィルタを設定して、内部ネットワーク上のポート 22 に対する外部からのアクセスを遮断します。

Affected Applications

Application Name
SSH

Advisory Publisher Entries

Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
CHECK Contains/SSH-[12]\..*/
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	DNS Available	Score	0
Published		Strategy	Network Reconnaissance
	nCircle: 1282	CVSS v2	0.0
CVSS v3	0.0		

Description

解説
Domain Name System つまり DNS は、異なるホスト、ネットワーク、プロトコルファミリ、インターネット、及び管理組T で名前を使用できるように、リソースに名前を付ける機構を提供するよう設計された情報システムです。
DNS はそれぞれ、ポート 53/TCP と 53/UDP を使用します。

技術的な詳細説明
DNS サーバーは、ネットワークに関する情報を調べることができます。
DNS サーバーは、誤って設定された場合にホスト名と内部 IP アドレスが明らかにされます。

解決策:
このホストで DNS が不必要な場合は、サービスを無効にしてください。無効にするには、該当する rc ファイル又は rc runlevel ファイルから DNS エントリを削除します (Windows で実行されている DNS を無効にするには、コントロールパネルの[サービス]を使用します)。

Affected Applications

Application Name
DNS TCP
DNS UDP

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
SEND Execute[\x7E\x27\x00\x00\x00\x00\x00\x00\x00\x00\x00] THEN CHECK Contains[\x7E\x27]
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	HTTP Available	Score	0
Published	nCircle: 1343	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

Hyper Text Transfer Protocol（HTTP）は、アプリケーションレベルのプロトコルで、Webサーバがインターネット経由の情報転送に使用します。

詳細
HTTPは、Webベースのアプリケーション間で情報のやり取りを行う方法を提供することから、特有のセキュリティ上のリスクが存在します。HTTPは、Web専用サーバ上でのみ、使用可能にすることをお勧めします。

解決策
HTTPがサーバ運用に必要なければ、使用不可に設定してください。

Affected Applications

Application Name
HTTP

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	E-Mail Services Available	Score	0
Published		Strategy	Network Reconnaissance
	nCircle: 1750	CVSS v2	0.0
CVSS v3	0.0		

Description

解説
メールサービスの稼動が確認されました。
実在するアカウント情報を推測できる可能性があります。

解決策
サーバの運用上、メールサービスが不要な場合は停止して下さい。
メールサービスが必要な場合は、特に対処する必要はありません。

Affected Applications

Application Name
IMAP
POP3
SMTP

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

STOP WITH Match
STOP WITH Match
STOP WITH Match Authentication Attempt

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	Untrusted SSL/TLS Certificate	Score	0
Published		Strategy	Network Reconnaissance
	nCircle: 26188	CVSS v2	0.0
CVSS v3	0.0		

Description

解説
このホストの SSL 証明書は、信頼できない認証局が署名したものです。ユーザーがこの証明書を使用するサイトを表示しようとした場合、ブラウザからこの接続は信頼できないという内容を通知されます。また、ユーザーがこのサイトを表示するためには、その証明書を例外として追加する必要があります。

解決策
証明書は、信頼できる認証局から入手してください。

Affected Applications

Application Name
SSL
SSLv3
STARTTLS Capable SMTP Server (TLSv1.0)
TLSv1

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
CHECK Contains[220] WITH Length[3],Offset[0] THEN SEND String[EHLO ip360.ncircle.com\x0d\x0a] THEN CHECK Conta
ins/250[ -]STARTTLS\x0d\x0a/ THEN SEND String[STARTTLS\x0d\x0a] THEN CHECK Contains[220] BEFORE Contains/Ready
to start TLS\x0d\x0a|SMTP server ready\x0d\x0a/ THEN EXECUTE{ import aspl_ssl
try:  s = aspl_ssl.newSSLSe
ssion(ssl_protocol="TLSv1") s.getServerCertificate() rule.STOP(not s.Server.isCertificateSignedByTrust
edCA())
except aspl_ssl.SSLException:  rule.STOP( False )
}
EXECUTE{ import aspl_ssl
try:  hostnames = [None] hostnames += env.target.VirtualHostnames
for ho
stname in hostnames:  s = aspl_ssl.newSSLSession(ssl_protocol="SSLv3", server_name=hostname) s.
getServerCertificate() if not s.Server.isCertificateSignedByTrustedCA():  rule.STOP(True)

rule.STOP(False)
except aspl_ssl.SSLException:  rule.STOP( False )
}
```

```
EXECUTE{ import aspl_ssl
try:  hostnames = [None] hostnames += env.target.VirtualHostnames
for ho
stname in hostnames:  s = aspl_ssl.newSSLSession(ssl_protocol="TLSv1", server_name=hostname) ru
le.RECONNECT() s.getServerCertificate() if not s.Server.isCertificateSignedByTrustedCA():
rule.STOP(True)
rule.STOP(False)
except aspl_ssl.SSLException:  rule.STOP(False)
}
EXECUTE{ import aspl_ssl
try:  s = aspl_ssl.newSSLSession(ssl_protocol="SSLv3") s.getServerCertificate
() rule.STOP(not s.Server.isCertificateSignedByTrustedCA())
except aspl_ssl.SSLException:  rule.STOP(
False )
}
EXECUTE{ import aspl_ssl
try:  s = aspl_ssl.newSSLSession(ssl_protocol="TLSv1") s.getServerCertificate
() rule.STOP(not s.Server.isCertificateSignedByTrustedCA())
except aspl_ssl.SSLException:  rule.STOP(
False )
}
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	NO SSH AUTHENTICATION ATTEMPTED (no credentials configured)	Score	0
Published	nCircle: 30535	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

解説
本VnE ManagerにはSSH認証情報が設定されていません。
Credential診断を実施するためには認証情報が必要となります。
Scan ProfileのCredentialsにてSSHのチェックボックスにチェックが入っているか確認してください。

なお、本指摘は脆弱性ではありません。
Credential診断を実施しない場合には下記解決策を実施する必要はありません。

解決策
認証情報を設定してください。認証情報の追加方法は以下を参照ください。

1. Discover: Credentials Management で new （新規） をクリックします。
2. 認証情報の種類(type)にてSSH(key)もしくはSSH(password)を選択します。
3.
SSH(key)の場合
・ Name ：任意の名前を入力します。
・ Username ：SSHでログインするためのユーザー名を入力します。
・ Private Key ：SSHでログインするための秘密鍵を入力します。
SSH(password)
・ Name ：任意の名前を入力します。
・ Username ：SSHでログインするためのユーザー名を入力します。
・ Password ：SSHでログインするためのパスワードを入力します。
4. (任意) 認証情報セットについて注釈を入力します (自由形式のテキスト)。
5. Submit (送信) をクリックします。
6. ネットワーク、またはネットワーク内の IP 空間に認証情報を関連付けます。
7. Scan ProfileのBasicタブのCredentialsにてSSHのチェックボックスにチェックを入れます。

※補足
2についてはssh（key）かssh(password)を設定してください。
6については、新規に作成した認証情報をクリックし、Network Binding欄から
Add/Modifyをクリックし、作成した認証情報を使用して診断するネットワークを
追加してください。

Affected Applications

Application Name
SSH

Advisory Publisher Entries

Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE { smbcreds = rule.env.target.getCredentialSet('SSH')
if smbcreds == []:  rule.STOP( True ) else:  rul
e.STOP( False ) }
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	SSL Certificate Information	Score	0
Published		Strategy	Network Reconnaissance
	nCircle: 64658	CVSS v2	0.0
CVSS v3	0.0		

Description

DESCRIPTION
SSL Certificate Information has been stored for this host. Please view the instance data or Information tab for more details.

Affected Applications

Application Name
SSL Protocol Version

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE {
ssl_cert_info = [ ('SSL Certificate Serial Number', 'ssl_cert_serialNumber'), ('SSL Signatu
re Algorithm','ssl_cert_tbsSignatureAlgorithm'), ('SSL Certificate Issuer','ssl_cert_issuer'), ('SSL C
ertificate Not Valid Before','ssl_cert_notBefore'), ('SSL Certificate Not Valid After','ssl_cert_notAfter'
), ('SSL Certificate Subject','ssl_cert_subject'), ('SSL Certificate Key Usage','ssl_cert_keyUsage'),
('SSL Certificate ext Key Usage','ssl_cert_extKeyUsage'), ('SSL Certificate MD5 Thumbprint','ssl_cert_
MD5thumbprint'), ('SSL Certificate SHA1 Thumbprint','ssl_cert_SHA1thumbprint'), ('SSL Certificate Publ
ic Key Size','ssl_cert_publicKeySize'), ] ssl_vuln_info = [ ('SSLv2 Weak Ciphers','sslv2_weak_ciphers'),
('SSLv3 Weak Ciphers','sslv3_weak_ciphers'), ('TLSv1 Weak Ciphers','tlsv1_weak_ciphers'), ]
if str(env
.target.getPendingHostData('ssl_cert_serialNumber')) != 'None':  rule.transcript = '' rule.transcript +
...
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	SSH CBC Mode Ciphers Enabled	Score	0
Published		Strategy	Access Control Breach
	nCircle: 78682	CVSS v2	0.0
CVSS v3	0.0		

Description

DESCRIPTION
CBC Mode Ciphers are enabled on the SSH Server.
SOLUTION
Disable CBC Mode Ciphers and use CTR Mode Ciphers

Affected Applications

Application Name
SSH

Advisory Publisher Entries

Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE { from aspl_env import getContextVariable
try:  test_data = getContextVariable('ssh_client_to_ser
ver_ciphers') + getContextVariable('ssh_server_to_client_ciphers') except KeyError:  rule.STOP(False)
for
item in test_data:  if item.endswith('-cbc'):  rule.STOP(True)
rule.STOP(False) }
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	SSL Server Supports CBC Ciphers for TLSv1	Score	0
Published	nCircle: 81370	Strategy	Data-Driven Attack
CVSS v3	0.0	CVSS v2	0.0

Description

解説
暗号ブロックチェーン(CBC)はBEAST攻撃に対して脆弱です。
BEAST攻撃はCBCモードを使用しているSSL及びTLSの脆弱性を利用する。

解決策
CBC暗号を使用している暗号スイートを無効にします。

Affected Applications

Application Name
TLSv1

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE{ import aspl_ssl import dp, HIC import struct import time
def verifyHandshake(r):  if len(r) < 42:
return False
# Ensure this is a TLSv1 Handshake packet if not r[0:3] == '\x16\x03\x01':
return False
# Ensure this is a server_hello response if not r[5] == '\x02':  return False
# Ensure server_hello is tlsv1 if not r[9:11] == '\x03\x01':  return False
return True

#CBC Ciphers weak_ciphers = dict() weak_ciphers['\x00\x06'] = 'TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (40-bit)' we
ak_ciphers['\x00\x07'] = 'TLS_RSA_WITH_IDEA_CBC_SHA (128-bit)' weak_ciphers['\x00\x08'] = 'TLS_RSA_EXPORT_WITH
_DES40_CBC_SHA (40-bit)' weak_ciphers['\x00\x09'] = 'TLS_RSA_WITH_DES_CBC_SHA (56-bit)' weak_ciphers['\x00\x0a
'] = 'TLS_RSA_WITH_3DES_EDE_CBC_SHA (192-bit)' weak_ciphers['\x00\x0b'] = 'TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SH
A (40-bit)' weak_ciphers['\x00\x0c'] = 'TLS_DH_DSS_WITH_DES_CBC_SHA (56-bit)' weak_ciphers['\x00\x0e'] = 'TLS_
...
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	SSL Certificate Key Length < 4096 bits	Score	0
Published	nCircle: 81880	Strategy	Access Control Breach
CVSS v3	0.0	CVSS v2	0.0

Description

解説
このホストで使用されるSSL証明書は、4096ビット未満の鍵長を利用しています。

解決策
ユーザーは、少なくとも4096ビットの鍵長を利用し、新しい証明書を生成する必要があります。

Affected Applications

Application Name
SSL Protocol Version

Advisory Publisher Entries

BugTraq: 62226	http://www.securityfocus.com/bid/62226
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE { import dp
try:  data = env.target.getPendingHostData('ssl_cert_publicKeySize')[1] except (KeyErr
or,TypeError):  rule.STOP(False)
hostnames = [None] hostnames += env.target.VirtualHostnames
for hostname
in hostnames:  for item in data:  try:  port, item, bits = item.split() if h
ostname:  portcheck = 'TCP(%s:%s):'  % (hostname, dp.getPort()) else:
portcheck = 'TCP(%s):'  % dp.getPort() if port != portcheck:  continue exc
ept IndexError:  continue try:  if int(item) < 4096:  rule.STOP(T
rue) except (ValueError, TypeError):  continue rule.STOP(False) }
```

```
EXECUTE { import dp
try:  data = env.target.getPendingHostData('ssl_cert_publicKeySize')[1] except (KeyEr
ror,TypeError):  rule.STOP(False) for item in data:  try:  port, item, bits = item.split()
if port != 'TCP(%s):'  % dp.getPort():  continue except IndexError:  continue try:  if
int(item) < 4096:  rule.STOP(True) except (ValueError, TypeError):  continue rule.S
TOP(False) }
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	SSL Certificate Key Length <= 2048 bits	Score	0
Published	nCircle: 81881	Strategy	Access Control Breach
CVSS v3	0.0	CVSS v2	0.0

Description

解説
このホストで使用されるSSL証明書は、2048ビット以下の鍵長を利用しています。

解決策
ユーザーは、2048ビット以上の鍵長を利用し、新しい証明書を生成する必要があります。

Affected Applications

Application Name
SSL Protocol Version

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE { import dp
try:  data = env.target.getPendingHostData('ssl_cert_publicKeySize')[1] except (KeyErr
or,TypeError):  rule.STOP(False)
hostnames = [None] hostnames += env.target.VirtualHostnames
for hostname
in hostnames:  for item in data:  try:  port, item, bits = item.split() if h
ostname:  portcheck = 'TCP(%s:%s):'  % (hostname, dp.getPort()) else:
portcheck = 'TCP(%s):'  % dp.getPort() if port != portcheck:  continue exc
ept IndexError:  continue try:  if int(item) <= 2048:  rule.STOP(
True) except (ValueError, TypeError):  continue rule.STOP(False) }
EXECUTE { import dp
try:  data = env.target.getPendingHostData('ssl_cert_publicKeySize')[1] except (KeyEr
ror,TypeError):  rule.STOP(False) for item in data:  try:  port, item, bits = item.split()
if port != 'TCP(%s):'  % dp.getPort():  continue except IndexError:  continue try:  if
int(item) <= 2048:  rule.STOP(True) except (ValueError, TypeError):  continue rule.
STOP(False) }
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	SSL Certificate Key Length <= 4096 bits	Score	0
Published	nCircle: 81882	Strategy	Access Control Breach
CVSS v3	0.0	CVSS v2	0.0

Description

解説
このホストで使用されるSSL証明書は、4098ビット以下の鍵長を利用しています。

解決策
ユーザーは、4098ビット以上の鍵長を利用し、新しい証明書を生成する必要があります。

Affected Applications

Application Name
SSL Protocol Version

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE { import dp
try:  data = env.target.getPendingHostData('ssl_cert_publicKeySize')[1] except (KeyErr
or,TypeError):  rule.STOP(False)
hostnames = [None] hostnames += env.target.VirtualHostnames
for hostname
in hostnames:  for item in data:  try:  port, item, bits = item.split() if h
ostname:  portcheck = 'TCP(%s:%s):'  % (hostname, dp.getPort()) else:
portcheck = 'TCP(%s):'  % dp.getPort() if port != portcheck:  continue exc
ept IndexError:  continue try:  if int(item) <= 4096:  rule.STOP(
True) except (ValueError, TypeError):  continue rule.STOP(False) }
EXECUTE { import dp
try:  data = env.target.getPendingHostData('ssl_cert_publicKeySize')[1] except (KeyEr
ror,TypeError):  rule.STOP(False) for item in data:  try:  port, item, bits = item.split()
if port != 'TCP(%s):'  % dp.getPort():  continue except IndexError:  continue try:  if
int(item) <= 4096:  rule.STOP(True) except (ValueError, TypeError):  continue rule.
STOP(False) }
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	TLSv1 Enabled	Score	0
Published	nCircle: 209315	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

DESCRIPTION
TLSv1 is enabled on this host. TLSv1 is known to have cryptographic weaknesses. It is recommended that later versions of TLS be used.
SOLUTION
Replace or reconfigure applications that use TLSv1 to only use newer protocols.

Affected Applications

Application Name
TLSv1

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: Released in ASPL 609 on 2015-04-07	http://www.tripwire.com/vert/?Released in ASPL 609 on 2015-04-07

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	TLSv1.1 Enabled	Score	0
Published	nCircle: 212615	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

DESCRIPTION
TLSv1.1 is enabled on this host. TLSv1.1 is known to have cryptographic weaknesses. It is recommended that later versions of TLS be used.
SOLUTION
Replace or reconfigure applications that use TLSv1.1 to only use newer protocols.

Affected Applications

Application Name
TLSv1.1

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: Released in ASPL 616 on 2015-05-26	http://www.tripwire.com/vert/?Released in ASPL 616 on 2015-05-26

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	RFC7525 - Insecure TLS Protocol Version Exposure (Strict TLS)	Score	0
Published	nCircle: 212905	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

DESCRIPTION
RFC7525 "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" has mandated that TLSv1 and TLSv1.1 should not be used in modern implementations and deployments. These protocols do not support the security features and cipher suites available in TLSv1.2.
SOLUTION
Disable all SSL/TLS protocol support prior to TLSv1.2. RFC7525 recommends the use of TLSv1.2 with support for strong cipher suites.

Affected Applications

Application Name
TLSv1
TLSv1.1

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: Released in ASPL 623 on 2015-07-09	http://www.tripwire.com/vert/?Released in ASPL 623 on 2015-07-09

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	RFC7525 - TLS Transition Exposure	Score	0
Published	nCircle: 213013	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

DESCRIPTION
RFC7525 "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" has mandated that strict TLS is preferred when supported by the upper protocol. The transition from unecrypted to encrypted communication creates an opportunity for such as plaintext injection and ssl stripping attacks designed to keep the communication in the clear. SMTP, POP3, IMAP, and FTP offer strict TLS implementations, which should be used according to RFC7525.
SOLUTION
Enable only mandatory strict TLS service on SMTP, POP3, IMAP, and FTP.

Affected Applications

Application Name
SMTP STARTTLS Capability
TLS Capable FTP Server
TLS Capable IMAP Server
TLS Capable POP3 Server

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: Released in ASPL 623 on 2015-07-09	http://www.tripwire.com/vert/?Released in ASPL 623 on 2015-07-09

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	RFC7525 First Cipher Preference Exposure	Score	0
Published	nCircle: 213234	Strategy	Access Control Breach
CVSS v3	0.0	CVSS v2	0.0

Description

DESCRIPTION
RFC7525 "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" states that servers must prefer TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 over weaker cipher suites even if it was not the first proposal from the client. The stronger TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher is also acceptable per the RFC.
SOLUTION
Refer to vendor documentation for instructions on how to configure TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as the preferred cipher on the server.

Affected Applications

Application Name
TLSv1.2

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: Released in ASPL 623 on 2015-07-09	http://www.tripwire.com/vert/?Released in ASPL 623 on 2015-07-09

Rules

```
EXECUTE { import aspl_env try:  dCiphers = aspl_env.getContextVariable("tlsv1.2_cipher_order") except KeyEr
ror:  rule.STOP(False)
rfc7525_Cipher1 = dict() rfc7525_Cipher1['\xC0\x2F'] = "TLS_ECDHE_RSA_WITH_AES_128_
GCM_SHA256" rfc7525_Cipher1['\xC0\x30'] = "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" if dCiphers[0] in rfc7525_Ci
pher1.keys():  rule.STOP(True) rule.STOP(False) }
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	RFC7525 - Insecure TLS Protocol Version Exposure (POP3)	Score	0
Published	nCircle: 214234	Strategy	Network Reconnaissance
CVSS v3	0.0	CVSS v2	0.0

Description

DESCRIPTION
RFC7525 "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" has mandated that TLSv1 and TLSv1.1 should not be used in modern implementations and deployments. These protocols do not support the security features and cipher suites available in TLSv1.2.
SOLUTION
Disable all SSL/TLS protocol support prior to TLSv1.2. RFC7525 recommends the use of TLSv1.2 with support for strong cipher suites.

Affected Applications

Application Name
TLS Capable POP3 Server (TLSv1)
TLS Capable POP3 Server (TLSv1.1)

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: Released in ASPL 623 on 2015-07-09	http://www.tripwire.com/vert/?Released in ASPL 623 on 2015-07-09

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	BIND Version	Score	0
Published		Strategy	Network Reconnaissance
	nCircle: 63	CVSS v2	0.0
CVSS v3	0.0		

Description

解説
BINDのバージョン情報が取得できます。デフォルトの設定では、バージョン情報の問い合わせに応答してしまいます。
悪意あるユーザが、入手した情報を基に更なる攻撃を試みる可能性があります。

解決策
BINDの設定ファイル(named.conf)を編集し、バージョン情報の問い合わせに返答しないように制御することを推奨します。その後、設定を反映させるためにnamedサービスを再起動して下さい。

【記述例】
```
options {
version ""任意の文字列""; # 記載した文字列をクライアントに返信、空白でも可
};
```

なお、「Versionサブステートメント」はBIND 8.2以降に追加されました。そのため、バージョン情報の問い合わせに対して、どのような情報(任意の文字列を含む)であっても返答することは、BIND 8.2以降を使用しているということを攻撃者が確認できるということはご注意下さい。
可能であれば、「Viewステートメント」を使用し、信頼のおけるホストからのみ、バージョン情報の問い合わせに応答するように設定して下さい。
「Versionサブステートメント」を使用する場合は、「Versionサブステートメント」の設定は不要です。

【記述例】
```
##### named.conf
view ""external-chaos"" CHAOS {
 match-clients { any; };
 recursion no;
 zone ""bind"" {
 type master;
 file ""bind.zone"";
 allow-query { バージョン情報を返答する信頼のおけるアドレス(ホストやネットワーク)を指定 ;
 };
};

view ""external"" IN {
 既存のゾーンを定義
};
```

continued on next page

```
##### bind zone
$TTL 86400
@ CH SOA example.kccs.co.jp. hostmaster.kccs.co.jp (
2009072700 ;
28800 ;
7200 ;
604800 ;
3600 ;
)
CH NS example.kccs.co.jp.
version CH TXT ""XXXX"" # 応答するバージョン情報を記載
```

Affected Applications

Application Name
DNS UDP

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
SEND Execute[\x00\x0A\x01\x00\x00\x01\x00\x00\x00\x00\x00\x07\x76\x65\x72\x73\x69\x6F\x6E\x04\x62\x69\x6E\
x64\x00\x00\x10\x00\x03] THEN CHECK Contains/(4|8|9)\./
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Vulnerability

Vulnerability Name	TLS RFC7627 Extended Master Secret Computation Not Supported	Score	0
Published	nCircle: 219282	Strategy	Access Control Breach
CVSS v3	0.0	CVSS v2	0.0

Description

DESCRIPTION
The TLS Extended Master Secret Extension (RFC7627) is not available. This extension provides for a more robust TLS handshake through an enhanced master secret computation process. This extension was specifically introduced to defend against the possibility of a TLS "Triple Handshake" attack as described in the RFC. In some deployments, the lack of this server extension can enable a malicious server to carry out a man-in-the-middle attack. Techniques have been documented for performing this attack when TLS-based authentication is used after a TLS renegotiation and in conjunction with a session resumption.
SOLUTION
Refer to vendor documentation for instructions on how to enable RFC5746 support.

Affected Applications

Application Name
SSL
TLSv1
TLSv1.1
TLSv1.2

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: Released in ASPL 643 on 2015-11-11	http://www.tripwire.com/vert/?Released in ASPL 643 on 2015-11-11

Rules

```
EXECUTE { import struct import aspl_ssl import aspl_env
strVersion = "TLSv1" strContextVar = "%s_EMS_Extensio
n_Exposure" % (strVersion) if aspl_ssl.supported_ssl_types.has_key(strVersion):  strVersionHex = aspl_ssl.s
upported_ssl_types[strVersion] else:  rule.STOP(False) # Unsupported protocol
all_ciphers = aspl_ssl.ssl3_
cipher.copy() # This is the entire cipher list which is copied so it can be modified dCiphers = dict()
alert_
close_notify = '\x15' + strVersionHex + '\x00\x02\x01\x00' s = aspl_ssl.newSSLSession(ssl_protocol=strVersion)
c = aspl_ssl.SSLClient(s) client_hello = c.makeHello(hello_protocol=strVersion,cipher_suites=all_ciphers, tls
_extensions="\x00\x17\x00\x00") s.sendRawPacket(client_hello)
iCount = 0 fServerHello = False fCert = False f
```

```
Kex = False fHelloDone = False fExposed = False while iCount<5:  iCount += 1 try:  recv = s.sock
et.recv() except EOFError:  continue lstRecords = aspl_ssl.getSSLRecords(recv) #strLogMessa
...
EXECUTE { import struct import aspl_ssl import aspl_env
strVersion = "TLSv1.1" strContextVar = "%s_EMS_Extens
ion_Exposure" % (strVersion) if aspl_ssl.supported_ssl_types.has_key(strVersion):  strVersionHex = aspl_ssl
.supported_ssl_types[strVersion] else:  rule.STOP(False) # Unsupported protocol
all_ciphers = aspl_ssl.ssl
3_cipher.copy() # This is the entire cipher list which is copied so it can be modified dCiphers = dict()
aler
t_close_notify = '\x15' + strVersionHex + '\x00\x02\x01\x00' s = aspl_ssl.newSSLSession(ssl_protocol=strVersio
n) c = aspl_ssl.SSLClient(s) client_hello = c.makeHello(hello_protocol=strVersion,cipher_suites=all_ciphers, t
ls_extensions="\x00\x17\x00\x00") s.sendRawPacket(client_hello)
iCount = 0 fServerHello = False fCert = False
fKex = False fHelloDone = False fExposed = False while iCount<5:  iCount += 1 try:  recv = s.so
cket.recv() except EOFError:  continue lstRecords = aspl_ssl.getSSLRecords(recv) #strLogMes
...
EXECUTE { import struct import aspl_ssl import aspl_env
strVersion = "TLSv1.2" strContextVar = "%s_EMS_Extens
ion_Exposure" % (strVersion) if aspl_ssl.supported_ssl_types.has_key(strVersion):  strVersionHex = aspl_ssl
.supported_ssl_types[strVersion] else:  rule.STOP(False) # Unsupported protocol
all_ciphers = aspl_ssl.ssl
3_cipher.copy() # This is the entire cipher list which is copied so it can be modified dCiphers = dict()
aler
t_close_notify = '\x15' + strVersionHex + '\x00\x02\x01\x00' s = aspl_ssl.newSSLSession(ssl_protocol=strVersio
n) c = aspl_ssl.SSLClient(s) client_hello = c.makeHello(hello_protocol=strVersion,cipher_suites=all_ciphers, t
ls_extensions="\x00\x17\x00\x00") s.sendRawPacket(client_hello)
iCount = 0 fServerHello = False fCert = False
fKex = False fHelloDone = False fExposed = False while iCount<5:  iCount += 1 try:  recv = s.so
cket.recv() except EOFError:  continue lstRecords = aspl_ssl.getSSLRecords(recv) #strLogMes
...
```

Hosts

Hostname	IP Address	Score
Name not in DNS	133.9.193.144	0

Vulnerability

Vulnerability Name	POP3 Available	Score	0
Published		Strategy	Network Reconnaissance
	nCircle: 929	CVSS v2	0.0
CVSS v3	0.0		

Description

POP3 (Post Office Protocol)はリモートメールアクセスプロトコルです。POP は“オフライン”メール処理をサポートするために設計されました。オフライン状態では、メールは(通常は共有)サーバーに配信され、パーソナルコンピュータユーザーがサーバーに接続されているメール“クライアント”プログラムを定期的に呼び出して、保留メールをすべてユーザー自身のマシンにダウンロードします。このサービスは、必要がない場合には使用不可にしてください。

Affected Applications

Application Name
POP3

Advisory Publisher Entries

Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
CHECK Contains/^\+OK Microsoft Exchange.*POP3 server/
CHECK Contains/^\+OK.*POP3.*server ready/
CHECK Contains/^\+OK/ THEN SEND Execute[ip360pop3test29] THEN CHECK Contains/^-ERR/
Authentication Attempt
CHECK Contains/^\+OK/ THEN SEND Execute[user ip360pop3test28] THEN CHECK Contains/^(\+OK|-ERR)/ THEN SEND Exec
ute[pass ip360test28pop3] THEN CHECK Contains/^(\+OK|-ERR)/
Authentication Attempt
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
heap-wu1.heap.phys.waseda.ac.jp	133.9.193.169	178

Applications

Service	Application	Hosts
DNS TCP	Bind 9 tcp DNS	1
DNS UDP	BIND 9.8 UDP	1
H.323		1
HTTP	HTTP Server	1
HTTP	HTTP-Based Application	1
HTTPS	HTTP Server	1
HTTPS	HTTP-Based Application	1
HTTPS	TLSv1	1
HTTPS	TLSv1.1	1
HTTPS	TLSv1.2	1
IPv4 Layer 4		2
Open TCP Port	N/A	1
POP3	Dovecot POP3	1
POP3	TLS Capable POP3 Server (TLSv1)	1
POP3	TLS Capable POP3 Server (TLSv1.1)	1
POP3	TLS Capable POP3 Server (TLSv1.2)	1
SMTP	Postfix 2.x	1
SSH	OpenSSH 6.4	1
SSH	OpenSSH 6.7	1

Audits

Network Name	Scan Profile Name		Audit Start	Audit End	Approx Hours Taken
2017_yamada-lab	TEST_Tripwire: Profile	Standard	07/20/2017 15:00	07/20/2017 15:16	00:15