

BALLOU
Hosting Intelligence
HIAB Security Report

Powered by Outpost24 AB
2016-05-10

Report Information.....
Executive Summary.....
Target Summary.....
Vulnerability Details.....

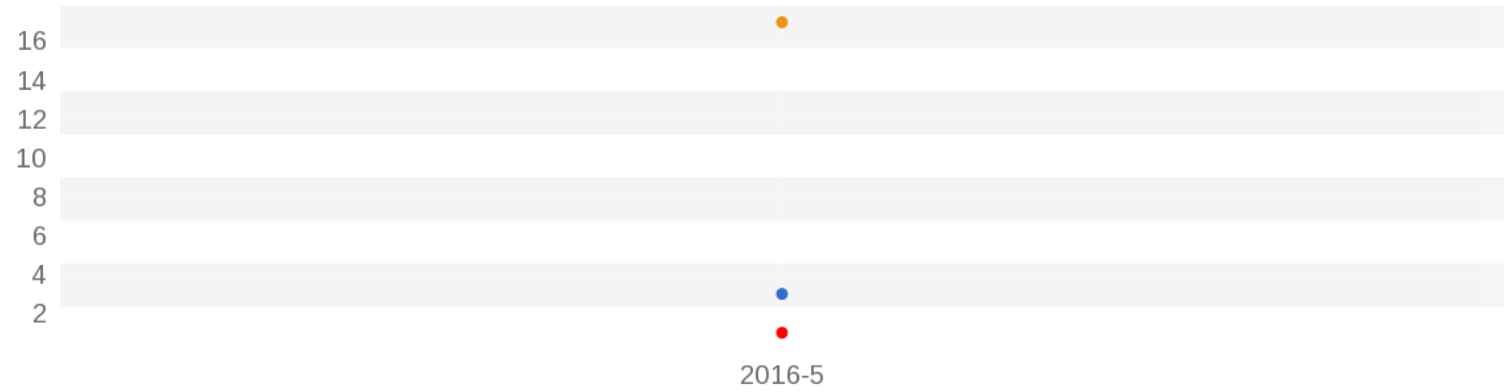
Report Information

Report type	Vulnerability
Report ID	2C91A18F5C73D472681BC8390C03DD6F
Date report was created	2016-05-10 10:21
Timezone for dates	GMT+2
Report created for	Ballou Internet Services AB
Report generated by	Daniel Gullin
Schedule job	TestScan
Scanning interval	2016-05-04 09:57 - 2016-05-04 10:14
Number of targets scanned	1
Number of risks found	21
Findings sorted by	CVSS
Reporting engine	4.1.140.24
Scanning engine	3.3.6
Rules database	2016-05-03 18:38
HIAB hardened	No

Executive Summary

Trend

Average number of findings for each risk level between 2015-05-04 and 2016-05-04

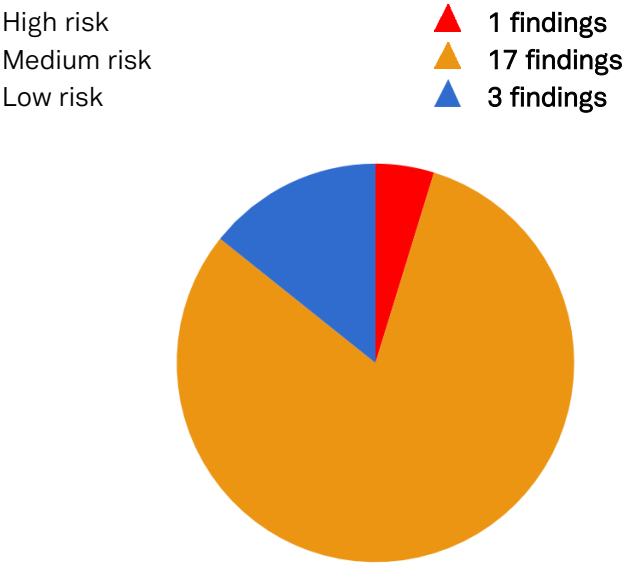


Remediation Trend

Average days of remediation for each risk level between 2015-05-04 and 2016-05-04

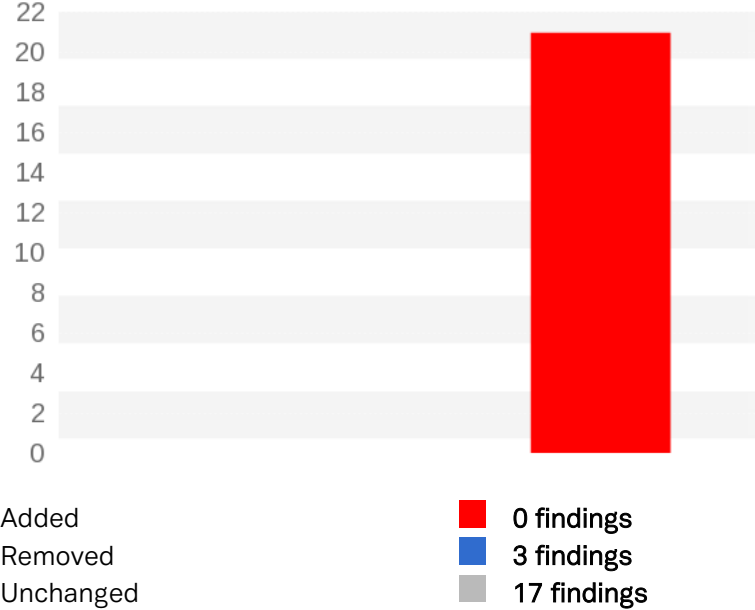


Risk Level Overview



Delta

Number of added and removed findings since last scan



Top 10 Solutions

Solution

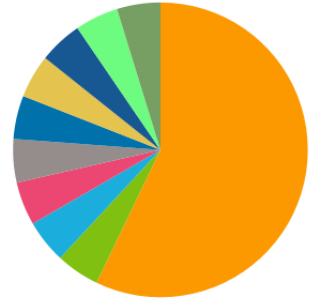
Upgrade to version 7.2p2 or later of OpenSSH
Require SMB Signatures
Disable TLSv1.0
Review certificate
Use stronger SSH ciphers
Disable MD5 for SSL/TLS
Disable weak SSL/TLS Ciphers
Use secure hash algorithms for certificates
Enable SMB Signatures
The vendor has not provided any solution yet

Open Issues

Targets

12
1
1
1
1
1
1
1
1
1

1
1
1
1
1
1
1
1
1
1

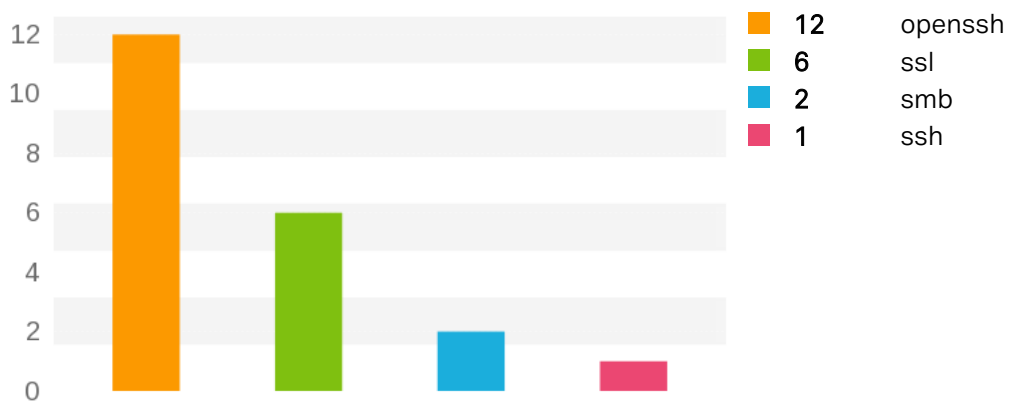


Vulnerabilities with Remediation age older than 90 days









Top 10 Risk Families

Overview for top 10 risk families



Target Summary

185.3.48.79

High risk	 1	Average CVSS score	5.0
Medium risk	 17	Scanning interval	2016-05-04 09:57 - 2016-05-04 10:14
Low risk	 3	Scan policy	Normal2
Open ports	22/TCP - ssh 135/TCP - emap 445/TCP - netbios-ssn 3389/TCP - ms-wbt-server 49152/TCP - dce/d95afe70-a6d5-4259-822e-2c84da1ddb0d 49153/TCP - dce/f6beaff7-1e19-4fbb-9f8f-b89e2018337c 49154/TCP - emap 49155/TCP - dce/367abb81-9844-35f1-ad32-98f038001003 49157/TCP - dce/12345778-1234-abcd-ef00-0123456789ac	Platform	Microsoft Windows Server 2008 R2 (6.1 SP1)
		Delta	 21 findings added  0 findings removed  0 findings unchanged

Vulnerability Details - 185.3.48.79

OpenSSH: Keyboard-interactive (MaxAuthTries bypass) Brute-force Authentication Protection Bypass

New finding

Risk factor	▲ High risk
CVSS score	8.5 - (AV:N/AC:L/Au:N/C:P/I:N/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, no impact to integrity of information and serious issues in rendering the system or information availability. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than or equal to 6.9
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
Reference	Vendor - http://www.openssh.com/ Solution - http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c Solution - http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c.diff?r1=1.42&r2=1.43&f=h
CVE	CVE-2015-5600
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1220768 - Added: 2015-08-05
Report date	2016-05-04 09:57

OpenSSH: Use-after-free local user privilege escalation vulnerability

New finding

Risk factor	▲ Medium risk
CVSS score	6.9 - (AV:L/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and local access to the system by an attacker who does not have access to credentials with full loss of confidentiality, full impact to the integrity of information and serious issues in rendering the system or information availability. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 7.0
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
Reference	Vendor - http://www.openssh.com/ Solution - https://github.com/openssh/openssh-portable/commit/5e75f5198769056089fb06c4d738ab0e5abc66f7 Solution - http://www.openssh.com/txt/release-7.0
CVE	CVE-2015-6564

Age 6 days - First seen: 2016-05-04 09:57
 Script ID 1221264 - Added: 2016-01-25
 Report date 2016-05-04 09:57

SSH Weak Ciphers

New finding

Risk factor ▲ Medium risk
CVSS score 6.4 - (AV:N/AC:L/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

This vulnerability can be exploited with ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.

Port 22/TCP - ssh
Family ssh
Product SSH

Description The remote SSH server allows communication with weak encryption ciphers. This may allow attackers to eavesdrop or disrupt communications.

Note: a cipher is considered to be weak if it uses a small key length or has known published attacks against it.

Information This finding was reported because (1) the following weak SSH ciphers were detected:

Encryption algorithm

- aes128-cbc
- 3des-cbc
- blowfish-cbc
- cast128-cbc
- aes192-cbc
- aes256-cbc
- arcfour
- rijndael-cbc@lysator.liu.se

Solution If you are using SSH Communications Security's Secure Shell, configure it to use a stronger cipher using the 'SSH Secure Shell for Windows Server Configuration.'

If you are using OpenSSH configure the Ciphers variable in /etc/sshd_config.

Category Workaround

Age 6 days - First seen: 2016-05-04 09:57
 Script ID 236727 - Added: 2010-04-06
 Report date 2016-05-04 09:57

SSL/TLS Weak and Export Ciphers Detected

New finding

Risk factor ▲ Medium risk
CVSS score 6.4 - (AV:N/AC:L/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

This vulnerability can be exploited with ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.

Port 3389/TCP - ms-wbt-server
Family ssl
Product SSL/TLS

Description The service running on this port allows the use of weak encryption ciphers, which might allow an attacker to eavesdrop on the communication.

Information

TLS1.0 Cipher Suite	OpenSSL Name	SNI Name
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	
TLS_RSA_WITH_RC4_128_MD5	RC4-MD5	

Solution For Apache, add the following line to the configuration file (e.g. httpd.conf):

SSLCipherSuite ALL:!MD5:!aNULL:!ADH:!eNULL:!LOW:!EXP:!RC4:+HIGH:+MEDIUM

and restart the server.

For Microsoft IIS 6.0:

1. Click Start, click Run, type regedit, and click OK.
2. In the Registry Editor browse to the following location:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers
3. Right click on the DES 56/56 key, select New, and click DWORD Value.
4. Name the key exactly as shown: Enabled
5. Verify that the key is set to type REG_DWORD with a Data value of 0x00000000 (0)
6. Repeat steps 3-5 for the following keys: NULL, RC2 40/120, RC2 56/128, RC4 40/128, RC4 56/128 and RC4 64/128
7. Reboot your server to force these changes to take effect.

For IIS 7.0/7.5

1. Open Microsoft Management Console and add the Group Policy Object Editor snap-in.
2. Expand Local Computer Policy -> Administrative Templates -> Network -> SSL Configuration Settings
3. Select SSL Cipher Suite Cipher and select Properties
4. Select Enabled under the Setting tab and paste the following into the SSL Cipher Suites box:

```
TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

5. Reboot your server to force these changes to take effect.

Category
Virtual hosts
Age
Script ID
Report date

Workaround
185.3.48.79
6 days - First seen: 2016-05-04 09:57
200845 - Added: 2007-07-07
2016-05-04 09:57

SMB Signing Disabled

New finding

Risk factor	▲ Medium risk
CVSS score	6.2 - (AV:A/AC:H/Au:N/C:C/I:C/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with advanced skills and access to an adjacent network by an attacker who does not have access to credentials with full loss of confidentiality, full impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	445/TCP - netbios-ssn
Family	smb
Product	SMB
Description	SMB signing is disabled on this server. Without SMB signing, an attacker could launch a man-in-the-middle attack against an SMBv1 connection. SMB signing will place a signature in each packet ensuring that SMB communications are not altered.
Solution	Enable SMB Signatures
Category	Reconfigure
Reference	Solution - http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html#id2560885 Solution - http://support.microsoft.com/kb/887429
Age	6 days - First seen: 2016-05-04 09:57
Script ID	287712 - Added: 2012-12-11
Report date	2016-05-04 09:57

SMB Signing Not Required

New finding

Risk factor	▲ Medium risk
CVSS score	6.2 - (AV:A/AC:H/Au:N/C:C/I:C/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with advanced skills and access to an adjacent network by an attacker who does not have access to credentials with full loss of confidentiality, full impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	445/TCP - netbios-ssn
Family	smb
Product	SMB
Description	SMB signing is not required on this server. Without SMB signing, an attacker could launch a man-in-the-middle attack against an SMBv1 connection. SMB signing will place a signature in each packet ensuring that SMB communications are not altered.
Solution	Require SMB Signatures
Category	Reconfigure
Reference	Solution - http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html#id2560885 Solution - http://support.microsoft.com/kb/887429
Age	6 days - First seen: 2016-05-04 09:57
Script ID	289181 - Added: 2013-02-15
Report date	2016-05-04 09:57

OpenSSH: sshd Configuration AcceptEnv Wildcard Handling Remote Restriction Bypass

New finding

Risk factor	▲ Medium risk
CVSS score	5.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	sshd in OpenSSH does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 6.6
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
CVE	CVE-2014-2532
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1206094 - Added: 2014-04-07
Report date	2016-05-04 09:57

OpenSSH: Client Rejected HostCertificate Handling Missing SSHFP Record Verification Weakness

New finding

Risk factor	▲ Medium risk
CVSS score	5.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	The verify_host_key function in sshconnect.c in the client in OpenSSH allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than or equal to 6.6
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
Reference	Vendor - http://www.openssh.com/ Solution - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=742513
CVE	CVE-2014-2653
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1206127 - Added: 2014-04-07
Report date	2016-05-04 09:57

SSL/TLS Certificate Validation Failure

New finding

Risk factor	▲ Medium risk
CVSS score	5.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	3389/TCP - ms-wbt-server
Family	ssl
Product	SSL/TLS
Description	We were unable to validate the certificate chain provided by this service. This may be because we were unable to find a valid host name for this target. Host names can be added under "Virtual Hosts" in the target configuration.
Information	185.3.48.79: cannot validate certificate for 185.3.48.79 because it doesn't contain any IP SANs
Solution	If the certificate is expired please renew the certificate. If the "Gathered Information" section does not contain a valid host name for the target, please add the host name to the target configuration. If the certificate chain could not be resolved to a trust anchor, please make sure the server passes the complete certificate chain up until a trust anchor. If the chain is still not verified and you are using an internal certificate authority, please add the certificates of that authority to the scan policy. If the certificate is not signed by a valid authority, please consider buying a trusted certificate or implementing your own public key infrastructure.
Category	Reconfigure
Virtual hosts	185.3.48.79
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1213134 - Added: 2015-02-13
Report date	2016-05-04 09:57

OpenSSH: sshd CRLF Injection Vulnerability

New finding

Risk factor	▲ Medium risk
CVSS score	5.5 - (AV:N/AC:L/Au:S/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with ease and network access to the system by an attacker with the possibility to log in once with some impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently openly or financially obtainable exploits on the market, or the attack is well described in the public domain.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 7.2p2
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
Reference	Vendor - http://www.openssh.com/ Solution - http://www.openssh.com/txt/x11fwd.adv Solution - http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/session.c.diff?r1=1.281&r2=1.282&f=h Solution - http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/session.c
CVE	CVE-2016-3115
Exploitability	Public exploit available

Age 6 days - First seen: 2016-05-04 09:57
 Script ID 1232107 - Added: 2016-03-24
 Report date 2016-05-04 09:57

SSL/TLS SHA1 Algorithm Certificate Signature Weakness

New finding

Risk factor ▲ Medium risk
CVSS score 5.0 - (AV:N/AC:L/Au:N/C:N/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

This vulnerability can be exploited with ease and network access to the system by an attacker who does not have access to credentials with no impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.

Port 3389/TCP - ms-wbt-server
Family ssl
Product SSL/TLS
Description The SHA1 algorithm is not considered safe for use in certificate signatures.
Information This finding was reported because (1) the detected SSL/TLS certificate signature algorithm was SHA1WithRSA

Solution Create a new certificate that is signed using a secure hashing algorithm such as SHA-256
Category Workaround
Bugtraq No Bugtraq
Virtual hosts 185.3.48.79
 Age 6 days - First seen: 2016-05-04 09:57
 Script ID 1213242 - Added: 2015-02-11
 Report date 2016-05-04 09:57

OpenSSH: ssh_packet_read_poll2 Function Denial of Service

New finding

Risk factor ▲ Medium risk
CVSS score 5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

This vulnerability can be exploited with ease and network access to the system by an attacker who does not have access to credentials with no impact on confidentiality, no impact to integrity of information and some impact on system or information availability. There are currently no exploits in the public domain. However, attacks may be well described or privately held.

Port 22/TCP - ssh
Family openssh
Product OpenSSH
Description The ssh_packet_read_poll2 function in packet.c in OpenSSH allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic.
Information This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 7.1p2
Solution Upgrade to version 7.2p2 or later of OpenSSH.
Category Update
Reference Vendor - <http://www.openssh.com/>
 Solution - <http://www.openssh.com/txt/release-7.1p2>
 Solution - <https://anongit.mindrot.org/openssh.git/commit?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0>

CVE CVE-2016-1907
 Age 6 days - First seen: 2016-05-04 09:57
 Script ID 1227388 - Added: 2016-01-25
 Report date 2016-05-04 09:57

OpenSSH: loggingrace / maxstartup Threshold Connection Saturation Remote DoS

New finding

Risk factor	▲ Medium risk
CVSS score	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with ease and network access to the system by an attacker who does not have access to credentials with no impact on confidentiality, no impact to integrity of information and some impact on system or information availability. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	The default configuration of OpenSSH enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than or equal to 6.1
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
CVE	CVE-2010-5107
Age	6 days - First seen: 2016-05-04 09:57
Script ID	289781 - Added: 2013-03-18
Report date	2016-05-04 09:57

SSL/TLS RC4 Algorithm Pseudo-random Character Generation Weakness Plaintext Content Disclosure

New finding

Risk factor	▲ Medium risk
CVSS score	4.3 - (AV:N/AC:M/Au:N/C:P/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, no impact to integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	3389/TCP - ms-wbt-server
Family	ssl
Product	SSL/TLS
Description	The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.
Information	This finding was reported because (1) RC4 was detected as supported encryption protocol.
Solution	The vendor has acknowledged the existence of this vulnerability, but not yet provided a solution. Contact the vendor for further information. It may be wise to disable or limit access to this service in the meantime
Category	No known solution
Reference	Vendor - http://tools.ietf.org/html/rfc6101 Solution - http://cr.yp.to/talks/2013.03.12/slides.pdf
CVE	CVE-2013-2566
Virtual hosts	185.3.48.79
Age	6 days - First seen: 2016-05-04 09:57
Script ID	289955 - Added: 2013-04-02
Report date	2016-05-04 09:57

TLSv1.0 Detected

New finding

Risk factor	▲ Medium risk
CVSS score	4.3 - (AV:N/AC:M/Au:N/C:P/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, no impact to integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	3389/TCP - ms-wbt-server
Family	ssl
Product	SSL/TLS
Description	TLS 1.0 is not considered strong cryptography since it has known issues in the following areas: <ul style="list-style-type: none"> i) Not protected against cipher-block chaining (CBC) attacks. ii) The initialization vector (IV) is not an explicit IV. iii) Padding errors are not handled correctly.
Information	This finding was reported because (1) TLSv1.0 was detected as supported encryption protocol.
Solution	Disable TLSv1.0
Category	Reconfigure
Reference	Vendor - http://tools.ietf.org/html/rfc6101 Advisory - https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information_Supplement_v1.pdf Advisory - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
Virtual hosts	185.3.48.79
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1222353 - Added: 2015-10-30
Report date	2016-05-04 09:57

OpenSSH: channels.c x11_open_helper() Function Untrusted X11 Connection Forwarding Timeout Bypass

New finding

Risk factor	▲ Medium risk
CVSS score	4.3 - (AV:N/AC:M/Au:N/C:N/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and network access to the system by an attacker who does not have access to credentials with no impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	The x11_open_helper function in channels.c in ssh in OpenSSH, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 6.9
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
Reference	Vendor - http://www.openssh.com/ Solution - https://anongit.mindrot.org/openssh.git/commit?h=V_6_9&id=1bf477d3cdf1a864646d59820878783d42357a1d Solution - http://www.openssh.com/txt/release-6.9
CVE	CVE-2015-5352
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1220767 - Added: 2015-08-05
Report date	2016-05-04 09:57

OpenSSH: libc/glob(3) resource exhaustion

New finding

Risk factor	▲ Medium risk
CVSS score	4.0 - (AV:N/AC:L/Au:S/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with ease and network access to the system by an attacker with the possibility to log in once with no impact on confidentiality, no impact to integrity of information and some impact on system or information availability. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than or equal to 5.8
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
CVE	CVE-2010-4755
Age	6 days - First seen: 2016-05-04 09:57
Script ID	252115 - Added: 2011-03-07
Report date	2016-05-04 09:57

SSL/TLS MD5 Algorithm Weakness

New finding

Risk factor	▲ Medium risk
CVSS score	4.0 - (AV:N/AC:H/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with advanced skills and network access to the system by an attacker who does not have access to credentials with some impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	3389/TCP - ms-wbt-server
Family	ssl
Product	SSL/TLS
Description	Since MD5's compression function is not a pseudorandom function (PRF), it does not conform to the security proof of HMAC and is therefore broken in theory. There have been no known attacks on MD5 cipher suites but it is recommended to move to a cipher suite that uses SHA-2 or SHA-3 PRF.
Information	This finding was reported because (1) MD5 was detected as supported encryption protocol.
Solution	For Apache, add the following line to the configuration file (e.g. httpd.conf): SSLCipherSuite ALL:!MD5:!aNULL:!ADH:!eNULL:!LOW:!EXP:!RC4+RSA:+HIGH:+MEDIUM and restart the server. For Microsoft IIS 6: Open regedit and navigate to: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5] Create DWORD value named 'Enabled' and set value data to '0' For Microsoft IIS 7/7.5: 1. Open Microsoft Management Console and add the Group Policy Object Editor snap-in. 2. Expand Local Computer Policy -> Administrative Templates -> Network -> SSL Configuration Settings

3. Select SSL Cipher Suite Cipher and select Properties

4. Select Enabled under the Setting tab and paste the following into the SSL Cipher Suites box:

```
TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

5. Reboot your server to force these changes to take effect.

Category	Workaround
Virtual hosts	185.3.48.79
Age	6 days - First seen: 2016-05-04 09:57
Script ID	236788 - Added: 2010-04-08
Report date	2016-05-04 09:57

OpenSSH: post-authentication resource exhaustion bug via GSSAPI

New finding

Risk factor	▲ Low risk
CVSS score	3.5 - (AV:N/AC:M/Au:S/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

This vulnerability can be exploited with relative ease and network access to the system by an attacker with the possibility to log in once with no impact on confidentiality, no impact to integrity of information and some impact on system or information availability. There are currently no exploits in the public domain. However, attacks may be well described or privately held.

Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	The <code>ssh_gssapi_parse_ename</code> function in <code>gss-serv.c</code> , when <code>gssapi-with-mic</code> authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 5.9
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
CVE	CVE-2011-5000
Age	6 days - First seen: 2016-05-04 09:57
Script ID	280686 - Added: 2012-04-05
Report date	2016-05-04 09:57

OpenSSH: ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure

New

finding

Risk factor	▲ Low risk
CVSS score	2.1 - (AV:L/AC:L/Au:N/C:P/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with ease and local access to the system by an attacker who does not have access to credentials with some impact on confidentiality, no impact to integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	ssh-keysign.c in ssh-keysign in OpenSSH on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 5.8p2
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
CVE	CVE-2011-4327
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1205094 - Added: 2014-02-04
Report date	2016-05-04 09:57

OpenSSH: sshd MONITOR_REQ_PWNAM Request Privilege Escalation

New finding

Risk factor	▲ Low risk
CVSS score	1.9 - (AV:L/AC:M/Au:N/C:N/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
	This vulnerability can be exploited with relative ease and local access to the system by an attacker who does not have access to credentials with no impact on confidentiality, some impact to the integrity of information and without affecting the availability of the information or system. There are currently no exploits in the public domain. However, attacks may be well described or privately held.
Port	22/TCP - ssh
Family	openssh
Product	OpenSSH
Description	The monitor component in sshd in OpenSSH on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.
Information	This vulnerability was identified because (1) the detected version of OpenSSH, 5.8, is less than 7.0
Solution	Upgrade to version 7.2p2 or later of OpenSSH.
Category	Update
Reference	Vendor - http://www.openssh.com/ Solution - https://github.com/openssh/openssh-portable/commit/d4697fe9a28dab7255c60433e4dd23cf7fce8a8b Solution - http://www.openssh.com/txt/release-7.0
CVE	CVE-2015-6563
Age	6 days - First seen: 2016-05-04 09:57
Script ID	1221199 - Added: 2015-08-25
Report date	2016-05-04 09:57

Products Installed

New finding

Port	General	
Family	misc	
Product	Unspecified	
Description	This finding lists all the products that were detected by the scanner during the scan.	
Information	Product	Version
	OpenSSH	5.8
	Microsoft Windows	6.1 SP1
Category	No known solution	
Age	6 days - First seen: 2016-05-04 09:57	
Script ID	1221985 - Added: 2015-09-30	
Report date	2016-05-04 09:57	

SMB Supplied Login Credentials Failed

New finding

Port	445/TCP - netbios-ssn
Family	smb
Product	SMB
Description	The SMB credentials provided did not allow the scan to successfully authenticate.
Information	Failed
Category	Not classified
Age	6 days - First seen: 2016-05-04 09:57
Script ID	289579 - Added: 2013-03-04
Report date	2016-05-04 09:57

Windows Terminal Service: Detection

New finding

Port	3389/TCP - ms-wbt-server
Family	microsoft
Product	Windows Terminal Service
Description	<p>The remote host is running Windows Terminal Service.</p> <p>Terminal Services allow a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).</p> <p>If an attacker gains a valid login and password, he may be able to use this service to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.</p> <p>Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.</p>
Information	This finding was reported because (1) Windows Terminal Service was detected.
Solution	Disable or remove Windows Terminal Service if you do not use it, or filter traffic to this service.
Category	Disable
Age	6 days - First seen: 2016-05-04 09:57
Script ID	111910 - Added: 2007-07-02
Report date	2016-05-04 09:57

OS Detection

New finding

Port	General
Family	os
Product	Operating System
Description	It was possible to determine operating system on the target host.
Information	Microsoft Windows Server 2008 R2 (6.1 SP1) Release: Standard Build: 7601 Kernel: NT 6.1
Category	Not classified
Age	6 days - First seen: 2016-05-04 09:57
Script ID	268043 - Added: 2011-11-15
Report date	2016-05-04 09:57

SSH Detection

New finding

Port	22/TCP - ssh
Family	ssh
Product	SSH
Description	The SSH server was detected.
Information	This finding was reported because (1) SSH was detected and (2) the following banner was presented by the service: SSH-2.0-OpenSSH_5.8
Category	Not classified
Age	6 days - First seen: 2016-05-04 09:57
Script ID	125898 - Added: 2007-07-02
Report date	2016-05-04 09:57

SSL/TLS Cipher Suite List

New finding

Port	3389/TCP - ms-wbt-server		
Family	ssl		
Product	SSL/TLS		
Description	The service running on this port supports the following cipher suites.		
Information	TLS1.0 Cipher Suite	OpenSSL Name	SNI Name
	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	
	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	
	TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	
	TLS_RSA_WITH_RC4_128_MD5	RC4-MD5	
Category	Not classified		
Virtual hosts	185.3.48.79		
Age	6 days - First seen: 2016-05-04 09:57		
Script ID	217099 - Added: 2009-02-26		
Report date	2016-05-04 09:57		

SSL/TLS Signature-Signing Algorithm

New finding

Port	3389/TCP - ms-wbt-server
Family	ssl
Product	SSL/TLS
Description	The SSL Signature Signing Algorithm. Digital signatures are used to verify that data is received from the correct sender. Your signature can only be generated using your private key but can be verified by anyone with your public key. If your private key is ever stolen someone else will be able to impersonate you and could send out malicious content with the trust that it's coming from you.
Information	Your signature is signed using the algorithm: sha1WithRSAEncryption
Category	Not classified
Virtual hosts	185.3.48.79
Age	6 days - First seen: 2016-05-04 09:57
Script ID	249067 - Added: 2010-09-15
Report date	2016-05-04 09:57

SSL/TLS Certificate Information

New finding

Port	3389/TCP - ms-wbt-server
Family	ssl
Product	SSL/TLS
Description	X.509 Certificate Information
Information	Certificate Issuer: Common Name: SCANTEST Certificate Subject: Common Name: SCANTEST Valid not before:2016-05-03T07:52:19Z Valid not after: 2016-11-02T07:52:19Z Key algorithm: RSA, 2048 bits Signature algorithm: SHA1WithRSA ---
Category	Not classified
Virtual hosts	185.3.48.79
Age	6 days - First seen: 2016-05-04 09:57
Script ID	200827 - Added: 2007-07-02
Report date	2016-05-04 09:57

SMB Native LanMan Information

New finding

Port	445/TCP - netbios-ssn
Family	smb
Description	Sending an authentication request to this host reveals the following information:
Information	Domain: WORKGROUP Native LanMan: Windows Server 2008 R2 Standard 6.1 Operating System: Windows Server 2008 R2 Standard 7601 Service Pack 1
Age	6 days - First seen: 2016-05-04 09:57
Script ID	125677 - Added: 2015-06-26
Report date	2016-05-04 09:57

DCE services

New finding

Port	135/TCP - emap
Family	smb
Description	DCE services running on this host:
Information	<p>Local DCERPC services:</p> <p>object uuid: 765294ba-60bc-48b8-92e9-89fd77769d91 uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d - version 1.0 unknown (unknown rpc service) local rpc service</p> <p>object uuid: 765294ba-60bc-48b8-92e9-89fd77769d91 uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d - version 1.0 unknown (unknown rpc service) local rpc service</p> <p>object uuid: b08669ee-8cb5-43a5-a017-84fe00000000 uuid: 76f226c3-ec14-4325-8a99-6a46348418af - version 1.0 unknown (unknown rpc service) local rpc service</p> <p>object uuid: b08669ee-8cb5-43a5-a017-84fe00000000 uuid: 76f226c3-ec14-4325-8a99-6a46348418af - version 1.0 unknown (unknown rpc service) local rpc service</p> <p>object uuid: 6d726574-7273-0076-0000-000000000000 uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0 unknown (unknown rpc service) annotation: Impl friendly name local rpc service</p> <p>object uuid: b08669ee-8cb5-43a5-a017-84fe00000001 uuid: 76f226c3-ec14-4325-8a99-6a46348418af - version 1.0 unknown (unknown rpc service) local rpc service</p> <p>object uuid: 00000000-0000-0000-0000-000000000000 uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 - version 1.0 svchost.exe (DHCP Client Service) annotation: DHCP Client LRPC Endpoint local rpc service</p> <p>object uuid: a9c69f15-03e3-46f3-925c-99fe1a156b76 uuid: 906b0ce0-c70b-1067-b317-00dd010662da - version 1.0 msdtc.exe (Distributed Transaction Coordinator) local rpc service</p> <p>object uuid: ab80dae8-8c26-4495-9e97-150a65651b49 uuid: 906b0ce0-c70b-1067-b317-00dd010662da - version 1.0 msdtc.exe (Distributed Transaction Coordinator) local rpc service</p> <p>object uuid: f16e39ec-b88c-445b-a9db-541d6be743cd uuid: 906b0ce0-c70b-1067-b317-00dd010662da - version 1.0 msdtc.exe (Distributed Transaction Coordinator) local rpc service</p> <p>object uuid: b7a96b3c-9c20-484d-b352-05a4922fb8bc uuid: 906b0ce0-c70b-1067-b317-00dd010662da - version 1.0 msdtc.exe (Distributed Transaction Coordinator) local rpc service</p> <p>object uuid: 00000000-0000-0000-0000-000000000000 uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0 lsass.exe (Security Account Manager) local rpc service</p> <p>object uuid: 00000000-0000-0000-0000-000000000000 uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0 lsass.exe (Security Account Manager) local rpc service</p>

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345678-1234-abcd-ef00-0123456789ab - version 1.0
lsass.exe (IPsec Services (Windows XP & 2003))
annotation: IPsec Policy agent endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 - version 1.0
unknown (unknown rpc service)
annotation: Spooler function endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: ae33069b-a2a8-46ee-a235-ddfd339be281 - version 1.0
unknown (unknown rpc service)
annotation: Spooler base remote object endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 4a452661-8290-4b36-8fbe-7f4093a94978 - version 1.0
unknown (unknown rpc service)
annotation: Spooler function endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: dd490425-5325-4565-b774-7e27d6c09c24 - version 1.0
unknown (unknown rpc service)
annotation: Base Firewall Engine API
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 - version 1.0
unknown (unknown rpc service)
annotation: Fw APIs
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 2fb92682-6599-42dc-ae13-bd2ca89bd11c - version 1.0
unknown (unknown rpc service)

annotation: Fw APIs
local rpc service

object uuid: 3bdb59a0-d736-4d44-9074-c1ee00000001
uuid: 24019106-a203-4642-b88d-82dae9158929 - version 1.0
unknown (unknown rpc service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 7ea70bcf-48af-4f6a-8968-6a440754d5fa - version 1.0
unknown (unknown rpc service)
annotation: NSI server endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 7ea70bcf-48af-4f6a-8968-6a440754d5fa - version 1.0
unknown (unknown rpc service)
annotation: NSI server endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 3473dd4d-2e88-4006-9cba-22570909dd10 - version 5.0
unknown (unknown rpc service)
annotation: WinHttp Auto-Proxy Service
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 3473dd4d-2e88-4006-9cba-22570909dd10 - version 5.0
unknown (unknown rpc service)
annotation: WinHttp Auto-Proxy Service
local rpc service

object uuid: 666f7270-6c69-7365-0000-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
local rpc service

object uuid: 6c637067-6569-746e-0000-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
local rpc service

object uuid: 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
uuid: 2eb08e3e-639f-4fba-97b1-14f878961076 - version 1.0
unknown (unknown rpc service)
local rpc service

object uuid: 736e6573-0000-0000-0000-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
local rpc service

object uuid: 736e6573-0000-0000-0000-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
local rpc service

object uuid: 736e6573-0000-0000-0000-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 - version 1.0
svchost.exe (Scheduler Service)

local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 1ff70682-0a51-30e8-076d-740be8cee98b - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 1ff70682-0a51-30e8-076d-740be8cee98b - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 1ff70682-0a51-30e8-076d-740be8cee98b - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f - version 1.0
svchost.exe (Scheduler Service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 86d35949-83c9-4044-b424-db363231fd0c - version 1.0
unknown (unknown rpc service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 86d35949-83c9-4044-b424-db363231fd0c - version 1.0
unknown (unknown rpc service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 86d35949-83c9-4044-b424-db363231fd0c - version 1.0
unknown (unknown rpc service)
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af - version 1.0
unknown (unknown rpc service)
annotation: IP Transition Configuration endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af - version 1.0
unknown (unknown rpc service)
annotation: IP Transition Configuration endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af - version 1.0
unknown (unknown rpc service)
annotation: IP Transition Configuration endpoint
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a - version 1.0
unknown (unknown rpc service)
annotation: XactSrv service
local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a - version 1.0
 unknown (unknown rpc service)
 annotation: XactSrv service
 local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a - version 1.0
 unknown (unknown rpc service)
 annotation: XactSrv service
 local rpc service

object uuid: 73736573-6f69-656e-6e76-000000000000
 uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
 unknown (unknown rpc service)
 annotation: Impl friendly name
 local rpc service

object uuid: 73736573-6f69-656e-6e76-000000000000
 uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
 unknown (unknown rpc service)
 annotation: Impl friendly name
 local rpc service

object uuid: 73736573-6f69-656e-6e76-000000000000
 uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
 unknown (unknown rpc service)
 annotation: Impl friendly name
 local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: 30b044a5-a225-43f0-b3a4-e060df91f9c1 - version 1.0
 unknown (unknown rpc service)
 local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: 30b044a5-a225-43f0-b3a4-e060df91f9c1 - version 1.0
 unknown (unknown rpc service)
 local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: 30b044a5-a225-43f0-b3a4-e060df91f9c1 - version 1.0
 unknown (unknown rpc service)
 local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: f6beaff7-1e19-4fbb-9f8f-b89e2018337c - version 1.0
 unknown (unknown rpc service)
 annotation: Event log TCPIP
 local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c - version 1.0
 unknown (unknown rpc service)
 annotation: NRP server endpoint
 local rpc service

object uuid: 00000000-0000-0000-0000-000000000000
 uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 - version 1.0
 unknown (unknown rpc service)
 annotation: DHCPv6 Client LRPC Endpoint
 local rpc service

DCERPC services available remotely:

[pipes]
 object uuid: 765294ba-60bc-48b8-92e9-89fd77769d91
 uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d - version 1.0
 unknown (unknown rpc service)
 remote rpc service
 netbios name: \\SCANTEST

object uuid: b08669ee-8cb5-43a5-a017-84fe00000000
 uuid: 76f226c3-ec14-4325-8a99-6a46348418af - version 1.0

unknown (unknown rpc service)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 1ff70682-0a51-30e8-076d-740be8cee98b - version 1.0
svchost.exe (Scheduler Service)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f - version 1.0
svchost.exe (Scheduler Service)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 86d35949-83c9-4044-b424-db363231fd0c - version 1.0
unknown (unknown rpc service)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af - version 1.0
unknown (unknown rpc service)
annotation: IP Transition Configuration endpoint
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a - version 1.0
unknown (unknown rpc service)
annotation: XactSrv service
remote rpc service
netbios name: \\SCANTEST

object uuid: 73736573-6f69-656e-6e76-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
remote rpc service
netbios name: \\SCANTEST

object uuid: 73736573-6f69-656e-6e76-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 30b044a5-a225-43f0-b3a4-e060df91f9c1 - version 1.0
unknown (unknown rpc service)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 30b044a5-a225-43f0-b3a4-e060df91f9c1 - version 1.0
unknown (unknown rpc service)
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000

uuid: f6beaff7-1e19-4fbb-9f8f-b89e2018337c - version 1.0
unknown (unknown rpc service)
annotation: Event log TCPIP
remote rpc service
netbios name: \\SCANTEST

object uuid: 00000000-0000-0000-0000-000000000000
uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c - version 1.0
unknown (unknown rpc service)
annotation: NRP server endpoint
remote rpc service
netbios name: \\SCANTEST

[tcp port 49152]
object uuid: 765294ba-60bc-48b8-92e9-89fd77769d91
uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d - version 1.0
unknown (unknown rpc service)
remote rpc service

[tcp port 49157]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: 12345778-1234-abcd-ef00-0123456789ac - version 1.0
lsass.exe (Security Account Manager)
remote rpc service

[tcp port 49155]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: 367abb81-9844-35f1-ad32-98f038001003 - version 2.0
unknown (unknown rpc service)
remote rpc service

[tcp port 49154]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: 86d35949-83c9-4044-b424-db363231fd0c - version 1.0
unknown (unknown rpc service)
remote rpc service

[tcp port 49154]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af - version 1.0
unknown (unknown rpc service)
annotation: IP Transition Configuration endpoint
remote rpc service

[tcp port 49154]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a - version 1.0
unknown (unknown rpc service)
annotation: XactSrv service
remote rpc service

[tcp port 49154]
object uuid: 73736573-6f69-656e-6e76-000000000000
uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 - version 1.0
unknown (unknown rpc service)
annotation: Impl friendly name
remote rpc service

[tcp port 49154]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: 30b044a5-a225-43f0-b3a4-e060df91f9c1 - version 1.0
unknown (unknown rpc service)
remote rpc service

[tcp port 49153]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: f6beaff7-1e19-4fbb-9f8f-b89e2018337c - version 1.0
unknown (unknown rpc service)
annotation: Event log TCPIP
remote rpc service

[tcp port 49153]
object uuid: 00000000-0000-0000-0000-000000000000
uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c - version 1.0
unknown (unknown rpc service)

annotation: NRP server endpoint
remote rpc service

Age 6 days - First seen: 2016-05-04 09:57
Script ID 200242 - Added: 2015-06-26
Report date 2016-05-04 09:57

SMB Login

New finding

Port 445/TCP - netbios-ssn
Family smb
Description This check attempts to login to the remote SMB service.
Information The following login attempts were successful:

- Null session [<blank> / <blank>]

Selected login type: Null session

Age 6 days - First seen: 2016-05-04 09:57
Script ID 217925 - Added: 2015-06-26
Report date 2016-05-04 09:57

Traceroute

New finding

Port General
Family misc
Description This check tries to determine the path; traceroute, between our attacker and your target host. This path may give an attacker valuable information about through which routers; hops, traffic passes through. This is not a vulnerability in itself it is merely considered information, however, an attacker could possibly use this information to determine what ISP you have and so forth.

Note:

The path is not static and will most likely change depending on from which host you perform the traceroute. There is also no way you can fix this problem as it involves changing configurations on all the hops along the way.

Information host[:dport]/protocol (3 hops)
1 172.16.2.1:63694/udp
2 91.189.40.129:62525/udp
3 185.3.48.79:49154/tcp [open]

Age 6 days - First seen: 2016-05-04 09:57
Script ID 125993 - Added: 2015-06-26
Report date 2016-05-04 09:57

Relative IP identification numbers

New finding

Port General
Family ip
Description The operating system running on this host uses a weak algorithm for selecting IP ID numbers. This enables a potential attacker to predict subsequent IP ID values.

A range of problems comes with this, such as an attacker being able to use this host as a zombie when port scanning, or being able to keep track of the amount of requests made to this server over a period of time.

Age 6 days - First seen: 2016-05-04 09:57
Script ID 125472 - Added: 2015-06-26
Report date 2016-05-04 09:57