PCI Scan Vulnerability Report

PCI Status

The following table highlights the overall compliance status and each individual system's compliance status. Following the table is a detailed report specifying each system and its specific vulnerabilities.

Overall PCI Status	FAIL

Live IP Address Scanned	PCI Status
50.116.105.215	FAIL

Report Summary	
Company:	UA NETWORKS LTD
Hosts in account	1
Hosts scanned	1
Hosts active	1
Scan date	July 28, 2018
Report date	July 28, 2018

Summary of Vulnerabilities

Vulnerabilities total:	125

by PCI Severity		
PCI Severity	**Vulnerabilities**	**Total**
High	19	19
Medium	14	14
Low	92	92
Total	125	125

Detailed Results

50.116.105.215

Vulnerabilities total:	125

Vulnerabilities (125)

Service detection — port 26 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313667
Category: Service detection
CVE ID:

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
An SMTP server is running on this port.

HTTP Methods Allowed (per directory) — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313640
Category: Web Servers
CVE ID:

THREAT:
This plugin determines which HTTP methods are allowed on various CGI directories.

IMPACT:
By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

SOLUTION:

RESULT:
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/error
/icons
/vz
/vz/cp
/vz/skins
/vz/skins/winxp.new

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/cgi-bin
/vz/cp

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/error
/icons
/vz
/vz/skins
/vz/skins/winxp.new

- Invalid/unknown HTTP methods are allowed on :

/cgi-bin
/vz/cp

ISC BIND 9 Zero-Length RDATA Section Denial of Service / Information Disclosure — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**8.5** (AV:N/AC:L/Au:N/C:P/I:N/A:C)
ID:	8313636
Category:	DNS
CVE ID:	CVE-2012-1667 BID : 53772 Other references { cert : 381699 }

THREAT:
The remote name server may be affected by a denial of service / information disclosure vulnerability.

IMPACT:
According to its self-reported version number, the remote installation of BIND does not properly handle resource records with a zero-length RDATA section, which may lead to unexpected outcomes, such as crashes of the affected server, disclosure of portions of memory, corrupted zone data, or other problems.

Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND 9.6-ESV-R7-P1 / 9.7.6-P1 / 9.8.3-P1 / 9.9.1-P1 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.3-P1

OpenSSH LoginGraceTime / MaxStartups DoS — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** (AV:N/AC:L/Au:N/C:N/I:N/A:P)
ID:	8313704
Category:	Denial of Service
CVE ID:	CVE-2010-5107 BID : 58162

THREAT:
The remote SSH service is susceptible to a remote denial of service attack.

IMPACT:
According to its banner, a version of OpenSSH earlier than version 6.2 is listening on this port. The default configuration of OpenSSH installs before 6.2 could allow a remote attacker to bypass the LoginGraceTime and MaxStartups thresholds by periodically making a large number of new TCP connections and thereby prevent legitimate users from gaining access to the service.

Note that this plugin has not tried to exploit the issue or detect whether the remote service uses a vulnerable configuration. Instead, it has simply checked the version of OpenSSH running on the remote host.

SOLUTION:
Upgrade to OpenSSH 6.2 and review the associated server configuration settings.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 6.2

SYN Scan — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313734
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 4643/tcp was found to be open

ISC BIND 9 RDATA Section Handling DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313742
Category:	DNS
CVE ID:	CVE-2013-4854 BID : 61479

THREAT:
The remote name server is prone to a denial of service attack.

IMPACT:
According to its self-reported version number, the remote installation of BIND can be forced to crash via specially crafted queries containing malformed 'rdata' contents.

Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

Further note that this vulnerability is being actively exploited at the time of this writing.

SOLUTION:
Upgrade to BIND version 9.9.3-S1-P1 / 9.9.3-P2 / 8.8.5-P2 or later, or apply the vendor-supplied patch.

In the case of development branches, such as 9.8.6rc1 / 9.9.4rc1 / 9.9.4-S1rc1, no patch is currently available.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.5-P2

SSH Protocol Versions Supported — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313622
Category:	General
CVE ID:	

THREAT:
A SSH server is running on the remote host.

IMPACT:
This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

SOLUTION:

RESULT:
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0

smtpscan SMTP Fingerprinting — port 465 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313653
Category:	SMTP problems
CVE ID:	

THREAT:
It is possible to fingerprint the remote mail server.

IMPACT:
smtpscan is a SMTP fingerprinting tool written by Julien Bordet. It identifies the remote mail server even if the banners were changed.

SOLUTION:

RESULT:

smtpscan was not able to reliably identify this server. It might be:
Exim 3.35
Exim 4.82
Exim 4.72
Exim 4.10
The fingerprint differs from these known signatures on 2 point(s)

If you know precisely what it is, please send this fingerprint
to smtp-signatures@nessus.org :
:550:250:500:250:501:250:501:214:501:550:500:500:500:250:250
220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 04:49:39 -0500

ISC BIND 9.7.x < 9.9.7-P1 / 9.10.x < 9.10.2-P2 Resolver DNSSEC Validation DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313641
Category:	DNS
CVE ID:	CVE-2015-4620 BID : 75588

THREAT:
The remote name server is affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the remote installation of BIND is potentially affected by a denial of service vulnerability, when configured as a recursive resolver with DNSSEC validation, due to an error that occurs during the validation of specially crafted zone data returned in an answer to a recursive query. A remote attacker can exploit this, by causing a query to be performed against a maliciously constructed zone, to crash the resolver.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to BIND version 9.9.7-P1 / 9.10.2-P2 or later.

Alternatively, as a workaround, disable DNSSEC validation by setting the 'dnssec-validation' option to no.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.7-P1

SSH Server Type and Version Information — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313619
Category:	Service detection
CVE ID:	

THREAT:
An SSH server is listening on this port.

IMPACT:
It is possible to obtain information about the remote SSH server by sending an empty authentication request.

SOLUTION:

RESULT:

SSH version : SSH-2.0-OpenSSH_5.3
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password

SYN Scan — port 587 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313720
Category: Port scanners
CVE ID:

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 587/tcp was found to be open

Device Type — port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313631
Category: General
CVE ID:

THREAT:
It is possible to guess the remote device type.

IMPACT:
Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

SOLUTION:

RESULT:
Remote device type : general-purpose
Confidence level : 59

ISC BIND 9 libdns Regular Expression Handling DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313707
Category:	DNS
CVE ID:	CVE-2013-2266 BID : 58736

THREAT:
The remote name server is prone to a denial of service attack.

IMPACT:
According to its self-reported version number, the remote installation of BIND can be forced to crash via memory exhaustion caused by specially crafted regular expressions.

Note this vulnerability only affects Unix and Unix-like systems when the application has been compiled to include regular expression support.

Further note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND 9.8.4-P2 / 9.8.5b2 / 9.9.2-P2 / 9.9.3b2 or later, or apply the vendor-supplied patch. Alternatively, the application can be recompiled without regular expression support as a workaround.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.4-P2

OpenSSH < 6.9 Multiple Vulnerabilities — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** (AV:N/AC:M/Au:N/C:N/I:P/A:N)
ID:	8313623
Category:	Misc.
CVE ID:	CVE-2015-5352 BID : 75525

THREAT:
The SSH server running on the remote host is affected by multiple vulnerabilities.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 6.9. It is, therefore, affected by the following vulnerabilities :

- A flaw exists within the x11_open_helper() function in the 'channels.c' file that allows connections to be permitted after 'ForwardX11Timeout' has expired. A remote attacker can exploit this to bypass timeout checks and XSECURITY restrictions. (CVE-2015-5352)

- Various issues were addressed by fixing the weakness in agent locking by increasing the failure delay, storing the salted hash of the password, and using a timing-safe comparison function.

- An out-of-bounds read error exists when handling incorrect pattern lengths. A remote attacker can exploit this to cause a denial of service or disclose sensitive information in the memory.

- An out-of-bounds read error exists when parsing the 'EscapeChar' configuration option.

SOLUTION:
Upgrade to OpenSSH 6.9 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 6.9

Apache HTTP Server Version — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313613
Category:	Web Servers
CVE ID:	

THREAT:
It is possible to obtain the version number of the remote Apache HTTP server.

IMPACT:
The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

SOLUTION:

RESULT:

URL : https://50.116.105.215:4643/
Version : unknown
backported : 0

ISC BIND 9.x < 9.9.9-P3 Options Sections DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** (AV:N/AC:L/Au:N/C:N/I:N/A:P)
ID:	8313642
Category:	DNS
CVE ID:	CVE-2016-2848 BID : 93814

THREAT:
The remote name server is affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the instance of ISC BIND running on the remote name server is 9.x prior to 9.9.9-P3. It is, therefore, affected by a denial of service vulnerability when handling malformed options sections. An unauthenticated, remote attacker can exploit this, via a specially crafted OPT resource record, to cause an assertion failure, resulting in a daemon exit.

SOLUTION:
Upgrade to ISC BIND version 9.9.9-P3 / 9.10.4-P3 / 9.11.0 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.9-P3 / 9.10.4-P3 / 9.11.0

ISC BIND 9 DNS RDATA Handling DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313639

Category:	DNS
CVE ID:	CVE-2012-5166 BID : 55852

THREAT:
The remote name server may be affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the remote installation of BIND can become locked up if certain combinations of RDATA are loaded into the server. Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND 9.6-ESV-R7-P4 / 9.6-ESV-R8 / 9.7.6-P4 / 9.7.7 / 9.8.3-P4 / 9.8.4 / 9.9.1-P4 / 9.9.2 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.3-P4

SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam) — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** (AV:N/AC:M/Au:N/C:N/I:P/A:N)
ID:	8313609
Category:	Misc.
CVE ID:	CVE-2015-4000 BID : 74733

THREAT:
The remote host allows SSH connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

IMPACT:
The remote SSH server allows connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time (depending on modulus size and attacker resources).
This allows an attacker to recover the plaintext or potentially violate the integrity of connections.

SOLUTION:
Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

RESULT:
The SSH server is vulnerable to the Logjam attack because :

It supports diffie-hellman-group1-sha1 key
exchange.

It supports diffie-hellman-group-exchange-sha1
key exchange and allows a moduli smaller than
or equal to 1024.

Note that only an attacker with nation-state level resources

can effectively make use of the vulnerability, and only
against sessions where the vulnerable key exchange
algorithms are used.

OS Identification — port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313659
Category:	General
CVE ID:	

THREAT:
It is possible to guess the remote operating system.

IMPACT:
Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

SOLUTION:

RESULT:

Remote operating system : Linux Kernel 3.10
Linux Kernel 3.5
Linux Kernel 3.8
Linux Kernel 3.9
Confidence level : 59
Method : SinFP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SSH:!:SSH-2.0-OpenSSH_5.3
ICMP:!::1:1:0:64:0::1:0:::0::1:X:X:X:X:X:X:X:X:X:1:0:64:14480:MSTNW:7:1:1
SinFP:
P1:B10113:F0x12:W14600:O0204ffff:M1460:
P2:B10113:F0x12:W14480:O0204ffff0402080affffffff4445414401030307:M1460:
P3:B10120:F0x04:W0:O0:M0
P4:61101_7_p=443R
HTTP:!:Server: cPanel

SMTP:!:220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 03:45:33 -0500

220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

The remote host is running one of these operating systems :
Linux Kernel 3.10
Linux Kernel 3.5
Linux Kernel 3.8
Linux Kernel 3.9

Service detection — port 80 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313662
Category: Service detection
CVE ID:

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A web server is running on this port.

No Credentials Provided — port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313626
Category: Settings

CVE ID:

THREAT:
Nessus was able to find common ports used for local checks, however, no credentails were provided in the scan policy.

IMPACT:
Nessus was unable to execute credentialed checks because no credentials were provided.

SOLUTION:

RESULT:
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.

Service detection — port 995 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313677
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A TLSv1 server answered on this port.

HTTP X-Frame-Options Response Header Usage — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313632
Category:	CGI abuses
CVE ID:	

THREAT:
The remote web server does not take steps to mitigate a class of web application vulnerabilities.

IMPACT:
The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

SOLUTION:
Set a properly configured X-Frame-Options header for all requested resources.

RESULT:

The following pages do not set a X-Frame-Options response header or set a permissive policy:

- https://50.116.105.215:4643/vz/cp
- https://50.116.105.215:4643/vz/cp/login-wrapper

OpenSSH < 7.5 — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:P/I:N/A:N
ID:	8313615
Category:	Misc.
CVE ID:	

THREAT:
The SSH server running on the remote host is affected by an information disclosure vulnerability.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 7.5. It is, therefore, affected by an information disclosure vulnerability :

- An unspecified timing flaw exists in the CBC padding oracle countermeasures, within the ssh and sshd functions, that allows an unauthenticated, remote attacker to disclose potentially sensitive information.
Note that the OpenSSH client disables CBC ciphers by default. However, sshd offers them as lowest-preference options, which will be removed by default in a future release. (VulnDB 144000)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to OpenSSH version 7.5 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.5

SYN Scan — port 143 / tcp / imap

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313717
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 143/tcp was found to be open

SYN Scan — port 2080 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313726
Category:	Port scanners

CVE ID:

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2080/tcp was found to be open

Service detection — port 143 / tcp / imap

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313664
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
An IMAP server is running on this port.

Service detection — port 2096 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313680
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A web server is running on this port through TLSv1.

SYN Scan — port 110 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313716
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 110/tcp was found to be open

POP Server Detection — port 995 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313658
Category:	Service detection
CVE ID:	

THREAT:
A POP server is listening on the remote port.

IMPACT:
The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

SOLUTION:
Disable this service if you do not use it.

RESULT:

Remote POP server banner :

+OK Dovecot ready.

OpenSSH < 7.3 Multiple Vulnerabilities — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313625
Category:	Misc.
CVE ID:	CVE-2015-8325, CVE-2016-6515, CVE-2016-6210 BID : 86187, 92212

THREAT:
The SSH server running on the remote host is affected by multiple vulnerabilities.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 7.3. It is, therefore, affected by multiple vulnerabilities :

- A local privilege escalation when the UseLogin feature is enabled and PAM is configured to read .pam_environment files from home directories. (CVE-2015-8325)

- A flaw exists that is due to the program returning shorter response times for authentication requests with overly long passwords for invalid users than for valid users. This may allow a remote attacker to conduct a timing attack and enumerate valid usernames.

(CVE-2016-6210)

- A denial of service vulnerability exists in the auth_password() function in auth-passwd.c due to a failure to limit password lengths for password authentication. An unauthenticated, remote attacker can exploit this, via a long string, to consume excessive CPU resources, resulting in a denial of service condition. (CVE-2016-6515)

- An unspecified flaw exists in the CBC padding oracle countermeasures that allows an unauthenticated, remote attacker to conduct a timing attack. (VulnDB 142343)

- A flaw exists due to improper operation ordering of MAC verification for Encrypt-then-MAC (EtM) mode transport MAC algorithms when verifying the MAC before decrypting any ciphertext. An unauthenticated, remote attacker can exploit this, via a timing attack, to disclose sensitive information. (VulnDB 142344)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to OpenSSH version 7.3 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.3

ISC BIND 9 Recursive Response DNAME Record Handling DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** (AV:N/AC:L/Au:N/C:N/I:N/A:P)
ID:	8313736
Category:	DNS
CVE ID:	CVE-2016-8864 BID : 94067

THREAT:
The remote name server is affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the instance of ISC BIND 9 running on the remote name server is affected by a denial of service vulnerability due to improper handling of a recursive response containing a DNAME record in the answer section. An unauthenticated, remote attacker can exploit this to cause an assertion failure and daemon exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to ISC BIND version 9.9.9-P4 / 9.9.9-S6 / 9.10.4-P4 / 9.11.0-P1 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.9-P4 / 9.9.9-S6 / 9.10.4-P4 / 9.11.0-P1

SYN Scan — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313711
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 22/tcp was found to be open

Service detection — port 993 / tcp / imap

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313674
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A TLSv1 server answered on this port.

Service detection — port 587 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313666
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
An SMTP server is running on this port.

Service detection — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313688
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
An SSLv3 server answered on this port.

OpenSSH < 7.2p2 X11Forwarding xauth Command Injection — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**5.5** (AV:N/AC:L/Au:S/C:P/I:P/A:N)
ID:	8313638
Category:	Misc.
CVE ID:	CVE-2016-3115 Other references { edb-id : 39569 }

THREAT:
The SSH server running on the remote host is affected by a security bypass vulnerability.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 7.2p2. It is, therefore, affected by a security bypass vulnerability due to improper sanitization of X11 authentication credentials. An authenticated, remote attacker can exploit this, via crafted credentials, to inject arbitrary xauth commands, resulting in gaining read and write access to arbitrary files, connecting to local ports, or performing further attacks on xauth itself. Note that exploiting this vulnerability requires X11Forwarding to have been enabled.

SOLUTION:
Upgrade to OpenSSH version 7.2p2 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.2p2

FTP Server Detection — port 21 / tcp / ftp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313695
Category:	Service detection
CVE ID:	

THREAT:
An FTP server is listening on a remote port.

IMPACT:
It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

SOLUTION:

RESULT:

The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 04:00. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.

Web Application Tests : Load Estimation — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313624
Category:	CGI abuses
CVE ID:	

THREAT:
Load estimation for web application tests.

IMPACT:
This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

SOLUTION:

RESULT:
Here are the estimated number of requests in miscellaneous modes

for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

blind SQL injection : S=72 SP=192 AP=192 SC=240 AC=240
directory traversal (extended test) : S=306 SP=816 AP=816 SC=1020 AC=1020
arbitrary command execution (time based) : S=36 SP=96 AP=96 SC=120 AC=120
local file inclusion : S=24 SP=64 AP=64 SC=80 AC=80
header injection : S=2 SP=2 AP=2 SC=2 AC=2
XML injection : S=6 SP=16 AP=16 SC=20 AC=20
script injection : S=1 SP=1 AP=1 SC=1 AC=1
blind SQL injection (4 requests) : S=24 SP=64 AP=64 SC=80 AC=80
on site request forgery : S=1 SP=1 AP=1 SC=1 AC=1
cross-site scripting (comprehensive test): S=126 SP=336 AP=336 SC=420 AC=420
HTTP response splitting : S=9 SP=9 AP=9 SC=9 AC=9
SQL injection : S=174 SP=464 AP=464 SC=580 AC=580
arbitrary command execution : S=132 SP=352 AP=352 SC=440 AC=440
cross-site scripting (extended patterns) : S=7 SP=7 AP=7 SC=7 AC=7
directory traversal : S=174 SP=464 AP=464 SC=580 AC=580
web code injection : S=6 SP=16 AP=16 SC=20 AC=20
injectable parameter : S=12 SP=32 AP=32 SC=40 AC=40
format string : S=12 SP=32 AP=32 SC=40 AC=40
SSI injection : S=18 SP=48 AP=48 SC=60 AC=60
HTML injection : S=5 SP=5 AP=5 SC=5 AC=5
unseen parameters : S=210 SP=560 AP=560 SC=700 AC=700
SQL injection (2nd order) : S=6 SP=16 AP=16 SC=20 AC=20
directory traversal (write access) : S=12 SP=32 AP=32 SC=40 AC=40
persistent XSS : S=24 SP=64 AP=64 SC=80 AC=80

All tests : S=1399 SP=3689 AP=3689 SC=4605 AC=4605

Here are the estimated number of requests in miscellaneous modes
for both methods (GET and POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

blind SQL injection : S=144 SP=384 AP=384 SC=480 AC=480
directory traversal (extended test) : S=612 SP=1632 AP=1632 SC=2040 AC=2040
arbitrary command execution (time based) : S=72 SP=192 AP=192 SC=240 AC=240
local file inclusion : S=48 SP=128 AP=128 SC=160 AC=160
header injection : S=4 SP=4 AP=4 SC=4 AC=4
XML injection : S=12 SP=32 AP=32 SC=40 AC=40
script injection : S=2 SP=2 AP=2 SC=2 AC=2
blind SQL injection (4 requests) : S=48 SP=128 AP=128 SC=160 AC=160
on site request forgery : S=2 SP=2 AP=2 SC=2 AC=2
cross-site scripting (comprehensive test): S=252 SP=672 AP=672 SC=840 AC=840
HTTP response splitting : S=18 SP=18 AP=18 SC=18 AC=18
SQL injection : S=348 SP=928 AP=928 SC=1160 AC=1160
arbitrary command execution : S=264 SP=704 AP=704 SC=880 AC=880
cross-site scripting (extended patterns) : S=14 SP=14 AP=14 SC=14 AC=14
directory traversal : S=348 SP=928 AP=928 SC=1160 AC=1160
web code injection : S=12 SP=32 AP=32 SC=40 AC=40
injectable parameter : S=24 SP=64 AP=64 SC=80 AC=80
format string : S=24 SP=64 AP=64 SC=80 AC=80
SSI injection : S=36 SP=96 AP=96 SC=120 AC=120
HTML injection : S=10 SP=10 AP=10 SC=10 AC=10
unseen parameters : S=420 SP=1120 AP=1120 SC=1400 AC=1400
SQL injection (2nd order) : S=12 SP=32 AP=32 SC=40 AC=40

directory traversal (write access) : S=24 SP=64 AP=64 SC=80 AC=80
persistent XSS : S=48 SP=128 AP=128 SC=160 AC=160

All tests : S=2798 SP=7378 AP=7378 SC=9210 AC=9210

Your mode : single, GET and POST, thorough tests, Paranoid.
Maximum number of requests : 2798

OpenSSH < 7.6 — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:P/A:N
ID:	8313618
Category:	Misc.
CVE ID:	CVE-2017-15906 BID : 101552

THREAT:
The SSH server running on the remote host is affected by a file creation restriction bypass vulnerability.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 7.6. It is, therefore, affected by a file creation restriction bypass vulnerability related to the 'process_open' function in the file 'sftp-server.c' that allows authenticated users to create zero-length files regardless of configuration.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to OpenSSH version 7.6 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.6

SYN Scan — port 53 / tcp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313714
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 53/tcp was found to be open

SYN Scan — port 443 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313718
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 443/tcp was found to be open

Additional DNS Hostnames — port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313635
Category: General
CVE ID:

THREAT:
Nessus has detected potential virtual hosts.

IMPACT:
Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

SOLUTION:
If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

RESULT:
The following hostnames point to the remote host :
- mail.escgroups.com
- webmail.escgroups.com

Service detection — port 2078 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313684
Category: Service detection
CVE ID:

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A web server is running on this port through TLSv1.

smtpscan SMTP Fingerprinting — port 26 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313652
Category:	SMTP problems
CVE ID:	

THREAT:
It is possible to fingerprint the remote mail server.

IMPACT:
smtpscan is a SMTP fingerprinting tool written by Julien Bordet. It identifies the remote mail server even if the banners were changed.

SOLUTION:

RESULT:

smtpscan was not able to reliably identify this server. It might be:
Exim 3.35
Exim 4.82
Exim 4.72
Exim 4.10
The fingerprint differs from these known signatures on 2 point(s)

If you know precisely what it is, please send this fingerprint
to smtp-signatures@nessus.org :
:550:250:500:250:501:250:501:214:501:550:500:500:500:250:250
220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 04:49:17 -0500

SYN Scan — port 2087 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313730
Category: Port scanners
CVE ID:

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2087/tcp was found to be open

Common Platform Enumeration (CPE) port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313706
Category: General
CVE ID:

THREAT:
It was possible to enumerate CPE names that matched on the remote system.

IMPACT:
By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

SOLUTION:

RESULT:

The remote operating system matched the following CPE's :

cpe:/o:linux:linux_kernel:3.10
cpe:/o:linux:linux_kernel:3.5
cpe:/o:linux:linux_kernel:3.8
cpe:/o:linux:linux_kernel:3.9

Following application CPE's matched on the remote system :

cpe:/a:openssl:openssl:1.0.1e-fips
cpe:/a:openbsd:openssh:5.3 -> OpenBSD OpenSSH 5.3
cpe:/a:modssl:mod_ssl:2.2.29
cpe:/a:apache:http_server:2.2.29
cpe:/a:isc:bind:9.8.2rc1:redhat

Service detection — port 465 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313673
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A TLSv1 server answered on this port.

SYN Scan — port 465 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313719
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 465/tcp was found to be open

ISC BIND Unsupported Version Detection — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**10.0** AV:N/AC:L/Au:N/C:C/I:C/A:C
ID:	8313737
Category:	DNS
CVE ID:	

THREAT:
The remote host is running an unsupported version of ISC BIND.

IMPACT:
According to its self-reported version number, the installation of ISC BIND running on the remote name server is 9.8.x or earlier. It is, therefore, no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

SOLUTION:
Upgrade to a version of ISC BIND that is currently supported.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6

Fixed version : 9.9.8 or higher
End of Support URL: https://www.isc.org/downloads/

ISC BIND 9.7.x < 9.9.7-P2 / 9.10.x < 9.10.2-P3 TKEY Query Handling Remote DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313628
Category:	DNS
CVE ID:	CVE-2015-5477 Other references { edb-id : 37721 }

THREAT:
The remote name server is affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the installation of ISC BIND on the remote name server is potentially affected by a denial of service vulnerability due to a REQUIRE assertion flaw that occurs while handling TKEY queries. A remote attacker can exploit this by using a specially crafted TKEY query to crash the daemon.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to BIND version 9.9.7-P2 / 9.10.2-P3 or later, or apply the patch referenced in the advisory.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.7-P2

ISC BIND 9.x < 9.9.9-P2 / 9.10.x < 9.10.4-P2 / 9.11.0a3 < 9.11.0b2 lwres Query DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** (AV:N/AC:M/Au:N/C:N/I:N/A:P)
ID:	8313629
Category:	DNS
CVE ID:	CVE-2016-2775 Other references { iava : 2017-A-0004 }

THREAT:
The remote name server is affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the installation of ISC BIND running on the remote name server is 9.x prior to 9.9.9-P2, 9.10.x prior to 9.10.4-P2, or 9.11.0 a3 prior to 9.11.0b2. It is, therefore, affected by an error in the lightweight resolver (lwres) protocol implementation when resolving a query name that, when combined with a search list entry, exceeds the maximum allowable length. An unauthenticated, remote attacker can exploit this to cause a segmentation fault, resulting in a denial of service condition. This issue occurs when lwresd or the the named 'lwres' option is enabled.

SOLUTION:
Upgrade to ISC BIND version 9.9.8-P3 / 9.9.8-S4 / 9.10.3-P3 or later.

Note that BIND 9 version 9.9.9-S3 is available exclusively for eligible ISC Support customers.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.9-P2

HTTP X-Content-Security-Policy Response Header Usage — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313740
Category:	CGI abuses
CVE ID:	

THREAT:
The remote web server does not take steps to mitigate a class of web application vulnerabilities.

IMPACT:
The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

SOLUTION:
Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

RESULT:

The following pages do not set a Content-Security-Policy frame-ancestors response header or set a permissive policy:

- https://50.116.105.215:4643/vz/cp
- https://50.116.105.215:4643/vz/cp/login-wrapper

HyperText Transfer Protocol (HTTP) Redirect Information — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313703
Category:	Web Servers
CVE ID:	

THREAT:
The remote web server redirects requests to the root directory.

IMPACT:
The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

SOLUTION:
Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

RESULT:

Request : https://50.116.105.215:4643/
HTTP response : HTTP/1.1 302 Found
Redirect to : https://esc.escgroups.com:4643/vz/cp/
Redirect type : 30x redirect

Request : https://50.116.105.215:4643/vz/cp/
HTTP response : HTTP/1.1 302 Not Found
Redirect to : https://esc.escgroups.com:4643/vz/cp
Redirect type : 30x redirect

Final page : https://50.116.105.215:4643/vz/cp
HTTP response : HTTP/1.1 200 OK

Service detection — port 25 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313668
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
An SMTP server is running on this port.

SYN Scan — port 26 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313713
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 26/tcp was found to be open

ISC BIND 9 Multiple DoS Vulnerabilities — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313649
Category:	DNS
CVE ID:	CVE-2014-8680, CVE-2014-8500 BID : 71590, 73191

THREAT:
The remote name server is affected by multiple denial of service vulnerabilities.

IMPACT:
According to its self-reported version number, the remote installation of BIND is affected by multiple denial of service vulnerabilities :

- A flaw exists within the Domain Name Service due to an error in the code used to follow delegations. A remote attacker, with a maliciously-constructed zone or query, could potentially cause the service to issue unlimited queries leading to resource exhaustion. (CVE-2014-8500)

- Multiple flaws exist with the GeoIP feature. These flaws could allow a remote attacker to cause a denial of service. Note these issues only affect the 9.10.x branch. (CVE-2014-8680)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to BIND version 9.9.6-P1 / 9.10.1-P1 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.6-P1

HTTP Server Type and Version — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313743
Category:	Web Servers
CVE ID:	

THREAT:
A web server is running on the remote host.

IMPACT:
This plugin attempts to determine the type and the version of the remote web server.

SOLUTION:

RESULT:
The remote web server type is :

Apache

Web Server Directory Enumeration — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313689
Category:	Web Servers
CVE ID:	Other references { owasp : OWASP-CM-006 }

THREAT:
It is possible to enumerate directories on the web server.

IMPACT:
This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

SOLUTION:

RESULT:

The following directories were discovered:
/cgi-bin, /error, /icons

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards

DNS Server BIND version Directive Remote Version Disclosure — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313697
Category:	DNS
CVE ID:	

THREAT:
It is possible to obtain the version number of the remote DNS server.

IMPACT:
The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

SOLUTION:
It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

RESULT:

Version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6

OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**7.5** AV:N/AC:L/Au:N/C:P/I:P/A:P
ID:	8313637
Category:	Misc.
CVE ID:	CVE-2016-1908

THREAT:
The SSH server running on the remote host is affected by a security bypass vulnerability.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 7.2. It is, therefore, affected by a security bypass vulnerability due to a flaw in ssh (1) that is triggered when it falls back from untrusted X11 forwarding to trusted forwarding when the SECURITY extension is disabled by the X server. This can result in untrusted X11 connections that can be exploited by a remote attacker.

SOLUTION:
Upgrade to OpenSSH version 7.2 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.2

SMTP Server Detection — port 587 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313647
Category: Service detection
CVE ID:

THREAT:
An SMTP server is listening on the remote port.

IMPACT:
The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

SOLUTION:
Disable this service if you do not use it, or filter incoming traffic to this port.

RESULT:

Remote SMTP server banner :

220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 03:45:13 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

External URLs — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313627
Category: Web Servers
CVE ID:

THREAT:
Links to external sites were gathered.

IMPACT:
Nessus gathered HREF links to external sites by crawling the remote web server.

SOLUTION:

RESULT:

1 external URL was gathered on this web server :
URL... - Seen on...

https://esc.escgroups.com:4643/vz/cp/restore-password - /vz/cp

DNS Server Detection — port 53 / tcp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313616
Category:	DNS
CVE ID:	

THREAT:
A DNS server is listening on the remote host.

IMPACT:
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

SOLUTION:
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

RESULT:
N/A

IMAP Service Banner Retrieval — port 993 / tcp / imap

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313701
Category:	Service detection
CVE ID:	

THREAT:
An IMAP server is running on the remote host.

IMPACT:
An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

SOLUTION:

RESULT:
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE AUTH=PLAIN AUTH=LOGIN] Dovecot ready.

SYN Scan — port 2077 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313723
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2077/tcp was found to be open

SYN Scan — port 2083 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313728
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2083/tcp was found to be open

POP3 Cleartext Logins Permitted — port 110 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** AV:N/AC:H/Au:N/C:P/I:N/A:N
ID:	8313655
Category:	Misc.
CVE ID:	

THREAT:
The remote POP3 daemon allows credentials to be transmitted in cleartext.

IMPACT:
The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

SOLUTION:
Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

RESULT:
The following cleartext methods are supported :
USER
SASL PLAIN LOGIN

ISC BIND 9.3.0 < 9.9.8-P3 / 9.9.x-Sx < 9.9.8-S4 / 9.10.x < 9.10.3-P3 Multiple DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**6.8** (AV:N/AC:L/Au:S/C:N/I:N/A:C)
ID:	8313708
Category:	DNS
CVE ID:	CVE-2015-8704, CVE-2015-8705

THREAT:
The remote name server is affected by multiple denial of service vulnerabilities.

IMPACT:
According to its self-reported version number, the installation of ISC BIND running on the remote name server is affected by multiple denial of service vulnerabilities :

- A denial of service vulnerability exists due to improper handling of certain string formatting options. An authenticated, remote attacker can exploit this, via a malformed Address Prefix List (APL) record, to cause an INSIST assertion failure and daemon exit.
(CVE-2015-8704)

- A denial of service vulnerability exists due to a failure to properly convert OPT records and ECS options to formatted text. A remote attacker can exploit this to cause a REQUIRE assertion failure and daemon exit.
Note that this issue only affects BIND 9.10.x.
(CVE-2015-8705)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to BIND version 9.9.8-P3 / 9.9.8-S4 / 9.10.3-P3 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.8-P3

OpenSSH < 6.6 Multiple Vulnerabilities — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**7.5** (AV:N/AC:L/Au:N/C:P/I:P/A:P)
ID:	8313699
Category:	Misc.
CVE ID:	CVE-2014-2532, CVE-2014-1692 BID : 66355, 65230

THREAT:
The SSH server on the remote host is affected by multiple vulnerabilities.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 6.6. It is, therefore, affected by the following vulnerabilities :

- A flaw exists due to a failure to initialize certain data structures when makefile.inc is modified to enable the J-PAKE protocol. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in a denial of service condition and potentially the execution of arbitrary code. (CVE-2014-1692)

- An error exists related to the 'AcceptEnv' configuration setting in sshd_config due to improper processing of wildcard characters. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to bypass intended environment restrictions.
(CVE-2014-2532)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to OpenSSH version 6.6 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 6.6

OpenSSH < 7.4 Multiple Vulnerabilities — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**7.5** (AV:N/AC:L/Au:N/C:P/I:P/A:P)
ID:	8313692
Category:	Misc.
CVE ID:	CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-10010 BID : 94975, 94977, 94972, 94968 Other references { edb-id : 40962 }

THREAT:
The SSH server running on the remote host is affected by multiple vulnerabilities.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 7.4. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists in ssh-agent due to loading PKCS#11 modules from paths that are outside a trusted whitelist.
A local attacker can exploit this, by using a crafted request to load hostile modules via agent forwarding, to execute arbitrary code. To exploit this vulnerability, the attacker would need to control the forwarded agent-socket (on the host running the sshd server) and the ability to write to the file system of the host running ssh-agent. (CVE-2016-10009)

- A flaw exists in sshd due to creating forwarded Unix-domain sockets with 'root' privileges whenever privilege separation is disabled. A local attacker can exploit this to gain elevated privileges.
(CVE-2016-10010)

- An information disclosure vulnerability exists in sshd within the realloc() function due leakage of key material to privilege-separated child processes when reading keys. A local attacker can possibly exploit this to disclose sensitive key material. Note that no such leak has been observed in practice for normal-sized keys, nor does a leak to the child processes directly expose key material to unprivileged users.
(CVE-2016-10011)

- A flaw exists in sshd within the shared memory manager used by pre-authenticating compression support due to a bounds check being elided by some optimizing compilers and due to the memory manager being incorrectly accessible when pre-authenticating compression is disabled. A local attacker can exploit this to gain elevated privileges. (CVE-2016-10012)

- A denial of service vulnerability exists in sshd when handling KEXINIT messages. An unauthenticated, remote attacker can exploit this, by sending multiple KEXINIT messages, to consume up to 128MB per connection.
(VulnDB 148976)

- A flaw exists in sshd due to improper validation of address ranges by the AllowUser and DenyUsers directives at configuration load time. A local attacker can exploit this, via an invalid CIDR address range, to gain access to restricted areas. (VulnDB 148977)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to OpenSSH version 7.4 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.4

Service detection — port 3306 / tcp / mysql

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313686

Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A MySQL server is running on this port.

Web Application Cookies Not Marked HttpOnly — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313650
Category:	Web Servers
CVE ID:	Other references { cwe : 811, 79, 750, 864, 751, 800, 931, 801, 928, 20, 712, 725, 990, 442, 809, 722, 711, 900, 74, 629 }

THREAT:
HTTP session cookies might be vulnerable to cross-site scripting attacks.

IMPACT:
The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

SOLUTION:
Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

RESULT:

The following cookie does not set the HttpOnly cookie flag :

Name : vzcpLang
Path : /
Value : en
Domain :
Version : 1
Expires : 01-Jan-2030 00:00:00 GMT

Comment :
Secure : 1
Httponly : 0
Port :

SMTP Server Detection — port 26 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313645
Category:	Service detection
CVE ID:	

THREAT:
An SMTP server is listening on the remote port.

IMPACT:
The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

SOLUTION:
Disable this service if you do not use it, or filter incoming traffic to this port.

RESULT:

Remote SMTP server banner :

220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 03:55:42 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

ISC BIND 9.7.0.x < 9.9.6-P2 DNSSEC Validation DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**5.4** (AV:N/AC:H/Au:N/C:N/I:N/A:C)
ID:	8313634
Category:	DNS
CVE ID:	CVE-2015-1349 BID : 72673

THREAT:
The remote name server is affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the remote installation of BIND is potentially affected by a denial of service vulnerability due to an error relating to DNSSEC validation and the managed-keys feature. A remote attacker can trigger an incorrect trust-anchor management scenario in which no key is ready for use, resulting in an assertion failure and daemon crash.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to BIND version 9.9.6-P2 or later.

Alternatively, as a workaround, do not use 'auto' for the dnssec-validation or dnssec-lookaside options and do not configure a managed-keys statement.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.6-P2

SYN Scan — port 80 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313715
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 80/tcp was found to be open

DNS Sender Policy Framework (SPF) Enabled — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313612
Category:	DNS
CVE ID:	

THREAT:
The remote domain publishes SPF records.

IMPACT:
The remote domain publishes SPF records. SPF (Sender Policy Framework) is a mechanism to let an organization specify their mail sending policy, such as which mail servers are authorized to send mail on its behalf.

SOLUTION:

RESULT:

The following SPF records could be extracted for escgroups.com:

v=spf1 +a +mx +ip4:50.116.105.215 ~all

Service detection — port 2083 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313682
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A web server is running on this port through TLSv1.

IMAP Service Banner Retrieval — port 143 / tcp / imap

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313700
Category:	Service detection
CVE ID:	

THREAT:
An IMAP server is running on the remote host.

IMPACT:
An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

SOLUTION:

RESULT:
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.

SYN Scan — port 995 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313722
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 995/tcp was found to be open

Patch Report — port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313696
Category:	General
CVE ID:	

THREAT:
The remote host is missing several patches.

IMPACT:
The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

SOLUTION:
Install the patches listed below.

RESULT:

. You need to take the following 2 actions :

[ISC BIND 9.x.x < 9.9.10-P1 / 9.10.x < 9.10.5-P1 / 9.11.x < 9.11.1-P1 Multiple Vulnerabilities (100996)]

+ Action to take : Upgrade to ISC BIND version 9.9.10-P1 / 9.9.10-S2 / 9.10.5-P1 / 9.10.5-S2 / 9.11.1-P1 or later. Note that BIND 9 versions 9.9.10-S2 and 9.10.5-S2 are available exclusively for eligible ISC Support customers.

+ Impact : Taking this action will resolve the following 24 different vulnerabilities :
CVE-2017-3141, CVE-2017-3140, CVE-2016-8864, CVE-2016-2848, CVE-2016-2775
CVE-2015-8705, CVE-2015-8704, CVE-2015-5986, CVE-2015-5722, CVE-2015-5477
CVE-2015-4620, CVE-2015-1349, CVE-2014-8680, CVE-2014-8500, CVE-2014-0591

CVE-2013-4854, CVE-2013-2266, CVE-2012-5689, CVE-2012-5688, CVE-2012-5166
CVE-2012-4244, CVE-2012-3868, CVE-2012-3817, CVE-2012-1667

[OpenSSH < 7.6 (103781)]

+ Action to take : Upgrade to OpenSSH version 7.6 or later.

+ Impact : Taking this action will resolve the following 20 different vulnerabilities :
CVE-2016-6515, CVE-2016-6210, CVE-2016-3115, CVE-2016-1908, CVE-2016-10012
CVE-2016-10011, CVE-2016-10010, CVE-2016-10009, CVE-2015-8325, CVE-2015-6565
CVE-2015-6564, CVE-2015-6563, CVE-2015-5600, CVE-2015-5352, CVE-2014-2532
CVE-2014-1692, CVE-2012-0814, CVE-2011-4327, CVE-2010-5107, CVE-2010-4478

SYN Scan — port 21 / tcp / ftp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313710
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 21/tcp was found to be open

Web Server Allows Password Auto-Completion — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313633
Category: Web Servers
CVE ID:

THREAT:
The 'autocomplete' attribute is not disabled on password fields.

IMPACT:
The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

SOLUTION:
Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

RESULT:
Page : /vz/cp
Destination Page: /vz/cp/login-wrapper

Page : /vz/cp/login-wrapper
Destination Page: /vz/cp/login-wrapper

SYN Scan — port 993 / tcp / imap

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313721
Category: Port scanners
CVE ID:

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 993/tcp was found to be open

TCP/IP Timestamps Supported — port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313709
Category:	General
CVE ID:	

THREAT:
The remote service implements TCP timestamps.

IMPACT:
The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

SOLUTION:

RESULT:
N/A

Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**2.1** (AV:L/AC:L/Au:N/C:P/I:N/A:N)
ID:	8313691
Category:	Misc.
CVE ID:	CVE-2011-4327 BID : 47691 Other references { secunia : 44347 }

THREAT:
Local attackers may be able to access sensitive information.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is earlier than 5.8p2. Such versions may be affected by a local information disclosure vulnerability that could allow the contents of the host's private key to be accessible by locally tracing the execution of the ssh-keysign utility. Having the host's private key may allow the impersonation of the host.

Note that installations are only vulnerable if ssh-rand-helper was enabled during the build process, which is not the case for *BSD, OS X, Cygwin and Linux.

SOLUTION:
Upgrade to Portable OpenSSH 5.8p2 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 5.8p2

SMTP Server Detection — port 25 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313644
Category:	Service detection
CVE ID:	

THREAT:
An SMTP server is listening on the remote port.

IMPACT:
The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

SOLUTION:
Disable this service if you do not use it, or filter incoming traffic to this port.

RESULT:

Remote SMTP server banner :

220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 03:45:33 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

ISC BIND 9 NSEC3-Signed Zone Handling DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** (AV:N/AC:H/Au:N/C:N/I:N/A:P)
ID:	8313611
Category:	DNS
CVE ID:	CVE-2014-0591 BID : 64801

THREAT:
The remote name server may be affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the remote installation of BIND is affected by a denial of service vulnerability. This issue exists due to the handling of queries for NSEC3-signed zones related to the memcpy() function in the 'name.c' file on authoritative nameservers.

Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND version 9.9.5 / 9.9.4-P2 / 9.8.7 / 9.8.6-P2 / 9.6-ESV-R11 / 9.6-ESV-R10-P2 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.6-P2

OpenSSH < 5.7 Multiple Vulnerabilities — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**7.5** (AV:N/AC:L/Au:N/C:P/I:P/A:P)
ID:	8313643
Category:	Misc.
CVE ID:	CVE-2012-0814, CVE-2010-4478 BID : 51702, 45304

THREAT:
The remote SSH service may be affected by multiple vulnerabilities.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is earlier than 5.7. Versions before 5.7 may be affected by the following vulnerabilities :

- A security bypass vulnerability because OpenSSH does not properly validate the public parameters in the J-PAKE protocol. This could allow an attacker to authenticate without the shared secret. Note that this issue is only exploitable when OpenSSH is built with J-PAKE support, which is currently experimental and disabled by default, and that Nessus has not checked whether J-PAKE support is indeed enabled. (CVE-2010-4478)

- The auth_parse_options function in auth-options.c in sshd provides debug messages containing authorized_keys command options, which allows remote, authenticated users to obtain potentially sensitive information by reading these messages. (CVE-2012-0814)

SOLUTION:
Upgrade to OpenSSH 5.7 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 5.7

POP Server Detection — port 110 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313657
Category:	Service detection
CVE ID:	

THREAT:
A POP server is listening on the remote port.

IMPACT:
The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

SOLUTION:
Disable this service if you do not use it.

RESULT:

Remote POP server banner :

+OK Dovecot ready.

OpenSSH < 7.0 Multiple Vulnerabilities — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**8.5** (AV:N/AC:L/Au:N/C:P/I:N/A:C)
ID:	8313698
Category:	Misc.
CVE ID:	CVE-2015-6564, CVE-2015-6563, CVE-2015-6565, CVE-2015-5600 BID : 75990, 76317, 76497 Other references { edb-id : 41173 }

THREAT:
The SSH server running on the remote host is affected by multiple vulnerabilities.

IMPACT:
According to its banner, the version of OpenSSH running on the remote host is prior to 7.0. It is, therefore, affected by the following vulnerabilities :

- A security bypass vulnerability exists in the kbdint_next_device() function in file auth2-chall.c that allows the circumvention of MaxAuthTries during keyboard-interactive authentication. A remote attacker can exploit this issue to force the same authentication method to be tried thousands of times in a single pass by using a crafted keyboard-interactive 'devices' string, thus allowing a brute-force attack or causing a denial of service. (CVE-2015-5600)

- A security bypass vulnerability exists in sshd due to improper handling of username data in MONITOR_REQ_PAM_INIT_CTX requests. A local attacker can exploit this, by sending a MONITOR_REQ_PWNAM request, to conduct an impersonation attack. Note that this issue only affects Portable OpenSSH. (CVE-2015-6563)

- A privilege escalation vulnerability exists due to a use-after-free error in sshd that is triggered when handling a MONITOR_REQ_PAM_FREE_CTX request. A local attacker can exploit this to gain elevated privileges.
Note that this issue only affects Portable OpenSSH.
(CVE-2015-6564)

- A local command execution vulnerability exists in sshd due to setting insecure world-writable permissions for TTYs. A local attacker can exploit this, by injecting crafted terminal escape sequences, to execute commands for logged-in users. (CVE-2015-6565)

SOLUTION:
Upgrade to OpenSSH 7.0 or later.

RESULT:

Version source : SSH-2.0-OpenSSH_5.3
Installed version : 5.3
Fixed version : 7.0

Service detection — port 2087 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313681
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A web server is running on this port through TLSv1.

Inconsistent Hostname and IP Address — port 0 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313608
Category:	Gain root remotely
CVE ID:	

THREAT:
The remote host's hostname is not consistent with DNS information.

IMPACT:
The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

SOLUTION:
Fix the reverse DNS or host file.

RESULT:
The host name 'esc.escgroups.com' does not resolve to an IP address

Service detection — port 2080 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313683
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A web server is running on this port through TLSv1.

SMTP Server Non-standard Port Detection — port 26 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**5.0** AV:N/AC:L/Au:N/C:N/I:P/A:N
ID:	8313630
Category:	Backdoors
CVE ID:	

THREAT:
The remote SMTP service is running on a non-standard port.

IMPACT:
This SMTP server is running on a non-standard port. This might be a backdoor set up by attackers to send spam or even control of a targeted machine.

SOLUTION:
Check and clean the configuration.

RESULT:

Banner : 220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 03:55:42 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

SYN Scan — port 3306 / tcp / mysql

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313733
Category: Port scanners
CVE ID:

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 3306/tcp was found to be open

SYN Scan — port 2086 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313729
Category: Port scanners
CVE ID:

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2086/tcp was found to be open

IMAP Service STARTTLS Command Support — port 143 / tcp / imap

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313621
Category:	Misc.
CVE ID:	

THREAT:
The remote mail service supports encrypting traffic.

IMPACT:
The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

SOLUTION:

RESULT:

Here is the IMAP server's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

---------- snip ----------
Subject Name:

Common Name: esc.escgroups.com
Email Address: ssl@esc.escgroups.com

Issuer Name:

Common Name: esc.escgroups.com
Email Address: ssl@esc.escgroups.com

Serial Number: 01 E1 60 3F F5

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 22 04:17:08 2018 GMT
Not Valid After: May 22 04:17:08 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A6 76 8F FE 2B BD 2C A1 8B 18 65 B5 9D C8 ED 86 40 60 71
AD 2F 06 5F 85 77 5C D9 B3 2B 23 0B D7 10 7E 1B BC 01 29 9D
1A 20 D7 D7 4C C6 16 6D DD D4 25 6A 62 99 23 96 CA DF 18 1E
68 0C D6 BE BD 3E D2 65 FE 7D 84 45 9A 40 02 97 66 32 19 EB
B5 81 78 CC 06 FC EB C3 58 E6 49 25 5E E9 BC 2E 96 8F 42 71
9D 09 79 FC DD C4 55 23 11 7E 8E 60 75 0E 91 44 93 DE 2C F5
A1 8A 39 8D 7A 93 C5 B3 22 B3 2F F4 DF BF 45 CA BA D7 71 CF
A5 12 29 D6 7B DA FA 44 36 18 55 6C 5E E6 B0 F3 3F D7 15 2F
91 1B 89 48 1A 1B EE 6E 44 29 65 08 8E 9B 90 4A C9 80 48 4A
AB 58 E3 F5 A3 88 FD 2D 5D D4 FB FD 32 78 CF A3 15 7C C5 0E
ED B4 AF E8 CC 07 81 F6 59 8A 2A 43 3A B4 70 3A 6A 0C BC 59
B6 37 54 DC 15 77 35 C1 3E 21 C8 12 DE 89 81 6D D7 D4 A0 6A
A7 80 79 CC DD E2 E6 31 DA 22 91 88 BE AB 98 0F 4F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 2A 47 8E 82 25 54 77 F1 99 B2 37 4B 6E 72 18 43 F5 32 37
E6 82 30 3B 19 24 B7 81 45 30 A9 6B 15 29 B0 40 6F B4 D1 51
6B 2E FC CD 77 CC 77 AA 65 C4 C2 44 6A 55 87 0C C6 07 CA C2
8F 1B 09 BD 9C A5 C8 77 6D 80 CD 1B 29 40 1C 4D 78 BF 77 60
A0 40 1C 96 33 18 A7 DC 31 33 C2 62 B8 D5 8E 68 6F CF 2F AC
03 03 10 29 F2 8C AB 61 BD 6F 0C CA 3E 09 C1 B5 06 C8 40 E4
86 61 43 24 C9 50 DD 07 FB 50 89 3B AB 36 2B FB B3 9A 64 66
FD 5F 86 E7 F7 15 13 85 C5 23 28 11 18 D8 BF EF 9E 42 A3 2E
4A E8 EB D5 60 C6 19 C7 5C 7D 0E 99 3B 31 31 18 3A 8D 82 41
FF 95 B5 FA CC EC 1E A5 DF 7D D9 DA 20 50 91 1D 64 F4 46 5E
D8 28 6D CF 3D 20 73 0B 5D C0 BB 79 0E 23 B2 4E 21 D9 0A A7
BA 4D B0 5C E5 17 82 AC 93 EE F9 38 3F 8F 66 48 0B D8 0F 20
7E 28 1A 69 CC BE B0 1C 81 67 65 99 5D 60 38 42 14

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: D6 04 D4 AB BB D9 D5 D5 54 CC FF FE 00 25 3F 45 C3 73 4A C1

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: D6 04 D4 AB BB D9 D5 D5 54 CC FF FE 00 25 3F 45 C3 73 4A C1

Extension: Basic Constraints (2.5.29.19)
Critical: 0

---------- snip ----------

ISC BIND 9 Multiple Denial of Service Vulnerabilities — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313648
Category:	DNS
CVE ID:	CVE-2012-3817, CVE-2012-3868 BID : 54658, 54659

THREAT:
The remote name server may be affected by multiple denial of service vulnerabilities.

IMPACT:
According to its self-reported version number, the remote installation of BIND is affected by multiple denial of service vulnerabilities :

- Under a heavy query load, the application may use uninitialized data structures related to failed query cache access. This error can cause the application to crash. Note this issue only affects the application when DNSSEC validation is enabled. (CVE-2012-3817)

- Under a heavy, incoming TCP query load, the application can be affected by a memory leak that can lead to decreased performance and application termination on systems that kill processes that are out of memory.
(CVE-2012-3868)

Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND 9.6-ESV-R7-P2 / 9.7.6-P2 / 9.8.3-P2 / 9.9.1-P2 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.3-P2

ISC BIND Assertion Error Resource Record RDATA Query Parsing Remote DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)

ID:	8313620
Category:	DNS
CVE ID:	CVE-2012-4244 BID : 55522

THREAT:
The remote name server may be affected by a denial of service vulnerability.

IMPACT:
According to its self-reported version number, the remote installation of BIND will exit with an assertion failure if a resource record with RDATA in excess of 65535 bytes is loaded and then subsequently queried. Note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND 9.6-ESV-R7-P3 / 9.6-ESV-R8 / 9.7.6-P3 / 9.7.7 / 9.8.3-P3 / 9.8.4 / 9.9.1-P3 / 9.9.2 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.3-P3

Service detection — port 21 / tcp / ftp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313660
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
An FTP server is running on this port.

ISC BIND 9.0.x < 9.9.7-P3 / 9.10.x < 9.10.2-P4 Multiple DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313690
Category:	DNS
CVE ID:	CVE-2015-5986, CVE-2015-5722

THREAT:
The remote name server is affected by multiple denial of service vulnerabilities.

IMPACT:
According to its self-reported version number, the installation of ISC BIND running on the remote name server is potentially affected by the following vulnerabilities :

- A denial of service vulnerability exists due to an assertion flaw that is triggered when parsing malformed DNSSEC keys. An unauthenticated, remote attacker can exploit this, via a specially crafted query to a zone containing such a key, to cause a validating resolver to exit. (CVE-2015-5722)

- A denial of service vulnerability exists in the fromwire_openpgpkey() function in openpgpkey_61.c that is triggered when the length of data is less than 1. An unauthenticated, remote attacker can exploit this, via a specially crafted response to a query, to cause an assertion failure that terminates named. (CVE-2015-5986)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

SOLUTION:
Upgrade to BIND version 9.9.7-P3 / 9.10.2-P4 or later.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.7-P3

SYN Scan — port 2078 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313724
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2078/tcp was found to be open

ISC BIND 9.x.x < 9.9.10-P1 / 9.10.x < 9.10.5-P1 / 9.11.x < 9.11.1-P1 Multiple Vulnerabilities — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**7.2** AV:L/AC:L/Au:N/C:C/I:C/A:C
ID:	8313735
Category:	DNS
CVE ID:	CVE-2017-3141, CVE-2017-3140 BID : 99089, 99088 Other references { edb-id : 42121 }

THREAT:
The remote name server is affected by multiple vulnerabilities.

IMPACT:
According to its self-reported version number, the instance of ISC BIND running on the remote name server is 9.x.x prior to 9.9.10-P1, 9.10.x prior to 9.10.5-P1, or 9.11.x prior to 9.11.1-P1. It is, therefore, affected by multiple vulnerabilities :

- A denial of service vulnerability exists when processing Response Policy Zone (RPZ) rule types. An unauthenticated, remote attacker can exploit this, via a specially crafted query, to cause an infinite loop condition that degrades the server's functionality.
(CVE-2017-3140)

- A privilege escalation vulnerability exists in the BIND installer for Windows due to using an unquoted service path. A local attacker can exploit this to gain elevated privileges provided that the host file system permissions allow this. Note that non-Windows builds and installations are not affected. (CVE-2017-3141)

SOLUTION:
Upgrade to ISC BIND version 9.9.10-P1 / 9.9.10-S2 / 9.10.5-P1 / 9.10.5-S2 / 9.11.1-P1 or later. Note that BIND 9 versions 9.9.10-S2 and 9.10.5-S2 are available exclusively for eligible ISC Support customers.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.9.10-P1

DNS Server Fingerprinting — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313705
Category: DNS
CVE ID:

THREAT:
It may be possible to fingerprint the remote DNS server.

IMPACT:
This script attempts to identify the remote DNS server type and version by sending various invalid requests to the remote DNS server and analyzing the error codes returned.

SOLUTION:

RESULT:

The remote name server could be fingerprinted as being :

ISC BIND 9.8.2

Service detection — port 443 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313685
Category: Service detection
CVE ID:

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A web server is running on this port through TLSv1.

Web Application Vulnerable to Clickjacking — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:P/A:N
ID:	8313614
Category:	Web Servers
CVE ID:	Other references { cwe : 693 }

THREAT:
The remote web server may fail to mitigate a class of web application vulnerabilities.

IMPACT:
The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

SOLUTION:
Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

RESULT:

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

- https://50.116.105.215:4643/vz/cp
- https://50.116.105.215:4643/vz/cp/login-wrapper

Service detection — port 110 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313663
Category:	Service detection
CVE ID:	

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
A POP3 server is running on this port.

SYN Scan — port 2096 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313732
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2096/tcp was found to be open

SYN Scan — port 2079 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313725
Category: Port scanners
CVE ID:

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2079/tcp was found to be open

HyperText Transfer Protocol (HTTP) Information — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313651
Category: Web Servers
CVE ID:

THREAT:
Some information about the remote HTTP configuration can be extracted.

IMPACT:
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

SOLUTION:

RESULT:

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Sat, 28 Jul 2018 13:06:06 GMT
Server: Apache
Location: https://esc.escgroups.com:4643/vz/cp/
Content-Length: 290
Connection: close
Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
The document has moved here.
<hr>
<address>Apache Server at esc.escgroups.com Port 4643</address>
</body></html>

SYN Scan — port 2095 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313731
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2095/tcp was found to be open

DNS Server hostname.bind Map Hostname Disclosure — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313656
Category: DNS
CVE ID:

THREAT:
The DNS server discloses the remote host name.

IMPACT:
It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

SOLUTION:
It may be possible to disable this feature. Consult the vendor's documentation for more information.

RESULT:

The remote host name is :

esc.escgroups.com

smtpscan SMTP Fingerprinting — port 587 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313654
Category: SMTP problems

CVE ID:

THREAT:
It is possible to fingerprint the remote mail server.

IMPACT:
smtpscan is a SMTP fingerprinting tool written by Julien Bordet. It identifies the remote mail server even if the banners were changed.

SOLUTION:

RESULT:

smtpscan was not able to reliably identify this server. It might be:
Exim 3.35
Exim 4.82
Exim 4.72
Exim 4.10
The fingerprint differs from these known signatures on 2 point(s)

If you know precisely what it is, please send this fingerprint
to smtp-signatures@nessus.org :
:550:250:500:250:501:250:501:214:501:550:500:500:500:250:250
220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 04:50:04 -0500

Service detection — port 22 / tcp / ssh

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:
ID: 8313661
Category: Service detection
CVE ID:

THREAT:
The remote service could be identified.

IMPACT:
Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

SOLUTION:

RESULT:
An SSH server is running on this port.

ISC BIND 9 DNS64 Handling DoS (CVE-2012-5689) — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** AV:N/AC:M/Au:N/C:N/I:N/A:P
ID:	8313610
Category:	DNS
CVE ID:	CVE-2012-5689 BID : 57556

THREAT:
The remote name server is prone to a denial of service attack.

IMPACT:
According to its self-reported version number, the remote installation of BIND can be forced to crash via maliciously crafted DNS requests.

Note that this vulnerability only affects installs using the 'dns64' configuration option. Further note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND 9.8.5 / 9.9.3 or later. Alternatively, disable DNS64 functionality via configuration options.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.5

SYN Scan — port 2082 / tcp /

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313727
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 2082/tcp was found to be open

SYN Scan — port 25 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313712
Category:	Port scanners
CVE ID:	

THREAT:
It is possible to determine which TCP ports are open.

IMPACT:
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

SOLUTION:
Protect your target with an IP filter.

RESULT:
Port 25/tcp was found to be open

DNS Server Version Detection — port 53 / tcp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:

ID:	8313693
Category:	DNS
CVE ID:	

THREAT:
Nessus was able to obtain version information on the remote DNS server.

IMPACT:
Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

SOLUTION:

RESULT:

DNS server answer for "version.bind" (over TCP) :

9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6

POP3 Service STLS Command Support — port 110 / tcp / pop3

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313739
Category:	Misc.
CVE ID:	

THREAT:
The remote mail service supports encrypting traffic.

IMPACT:
The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

SOLUTION:

RESULT:

Here is the POP3 server's SSL certificate that Nessus was able to
collect after sending a 'STLS' command :

---------- snip ----------
Subject Name:

Common Name: esc.escgroups.com
Email Address: ssl@esc.escgroups.com

Issuer Name:

Common Name: esc.escgroups.com
Email Address: ssl@esc.escgroups.com

Serial Number: 01 E1 60 3F F5

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 22 04:17:08 2018 GMT
Not Valid After: May 22 04:17:08 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A6 76 8F FE 2B BD 2C A1 8B 18 65 B5 9D C8 ED 86 40 60 71
AD 2F 06 5F 85 77 5C D9 B3 2B 23 0B D7 10 7E 1B BC 01 29 9D
1A 20 D7 D7 4C C6 16 6D DD D4 25 6A 62 99 23 96 CA DF 18 1E
68 0C D6 BE BD 3E D2 65 FE 7D 84 45 9A 40 02 97 66 32 19 EB
B5 81 78 CC 06 FC EB C3 58 E6 49 25 5E E9 BC 2E 96 8F 42 71
9D 09 79 FC DD C4 55 23 11 7E 8E 60 75 0E 91 44 93 DE 2C F5
A1 8A 39 8D 7A 93 C5 B3 22 B3 2F F4 DF BF 45 CA BA D7 71 CF
A5 12 29 D6 7B DA FA 44 36 18 55 6C 5E E6 B0 F3 3F D7 15 2F
91 1B 89 48 1A 1B EE 6E 44 29 65 08 8E 9B 90 4A C9 80 48 4A
AB 58 E3 F5 A3 88 FD 2D 5D D4 FB FD 32 78 CF A3 15 7C C5 0E
ED B4 AF E8 CC 07 81 F6 59 8A 2A 43 3A B4 70 3A 6A 0C BC 59
B6 37 54 DC 15 77 35 C1 3E 21 C8 12 DE 89 81 6D D7 D4 A0 6A
A7 80 79 CC DD E2 E6 31 DA 22 91 88 BE AB 98 0F 4F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 2A 47 8E 82 25 54 77 F1 99 B2 37 4B 6E 72 18 43 F5 32 37
E6 82 30 3B 19 24 B7 81 45 30 A9 6B 15 29 B0 40 6F B4 D1 51
6B 2E FC CD 77 CC 77 AA 65 C4 C2 44 6A 55 87 0C C6 07 CA C2
8F 1B 09 BD 9C A5 C8 77 6D 80 CD 1B 29 40 1C 4D 78 BF 77 60
A0 40 1C 96 33 18 A7 DC 31 33 C2 62 B8 D5 8E 68 6F CF 2F AC
03 03 10 29 F2 8C AB 61 BD 6F 0C CA 3E 09 C1 B5 06 C8 40 E4
86 61 43 24 C9 50 DD 07 FB 50 89 3B AB 36 2B FB B3 9A 64 66
FD 5F 86 E7 F7 15 13 85 C5 23 28 11 18 D8 BF EF 9E 42 A3 2E
4A E8 EB D5 60 C6 19 C7 5C 7D 0E 99 3B 31 31 18 3A 8D 82 41
FF 95 B5 FA CC EC 1E A5 DF 7D D9 DA 20 50 91 1D 64 F4 46 5E
D8 28 6D CF 3D 20 73 0B 5D C0 BB 79 0E 23 B2 4E 21 D9 0A A7
BA 4D B0 5C E5 17 82 AC 93 EE F9 38 3F 8F 66 48 0B D8 0F 20
7E 28 1A 69 CC BE B0 1C 81 67 65 99 5D 60 38 42 14

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: D6 04 D4 AB BB D9 D5 D5 54 CC FF FE 00 25 3F 45 C3 73 4A C1

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: D6 04 D4 AB BB D9 D5 D5 54 CC FF FE 00 25 3F 45 C3 73 4A C1

Extension: Basic Constraints (2.5.29.19)
Critical: 0

---------- snip ----------

DNS Server Detection — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313617
Category:	DNS
CVE ID:	

THREAT:
A DNS server is listening on the remote host.

IMPACT:
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

SOLUTION:
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

RESULT:
N/A

ISC BIND 9 DNS64 Handling DoS — port 53 / udp / dns

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

PASS

VULNERABILITY DETAILS

CVSS Base Score:	**7.8** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
ID:	8313738
Category:	DNS
CVE ID:	CVE-2012-5688 BID : 56817

THREAT:
The remote name server is prone to a denial of service attack.

IMPACT:
According to its self-reported version number, the remote installation of BIND can be forced to crash via maliciously crafted DNS requests.

Note that this vulnerability only affects installs using the 'dns64' configuration option. Further note that Nessus has only relied on the version itself and has not attempted to determine whether or not the install is actually affected.

SOLUTION:
Upgrade to BIND 9.8.4-P1 / 9.9.2-P1 or later. Alternatively, disable DNS64 functionality via configuration options.

RESULT:

Installed version : 9.8.2rc1-RedHat-9.8.2-0.68.rc1.el6
Fixed version : 9.8.4-P1

CGI Generic Injectable Parameter Weakness — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313694
Category:	CGI abuses
CVE ID:	Other references { cwe : 86 }

THREAT:
Some CGIs are candidate for extended injection tests.

IMPACT:
Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

SOLUTION:

RESULT:

Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'LoginUser' parameter of the /vz/cp/login-wrapper CGI :

/vz/cp/login-wrapper?LoginUser=mwszgs

-------- output --------
<td><img src="/vz/skins/winxp.new/images/1x1.gif" width="10" heigh [...]
<td width="40%">Username</td>
<td align="left" width="60%"><input type="text" name="LoginUser" class="
FlatInput" title="Username" value="mwszgs"></td>
</tr>
<tr>

/vz/cp/login-wrapper?js_mode=0&LoginPass=&LoginUser=mwszgs&active_lang=d
efault&doLogin=Log%20in&java_mode='notdef'

-------- output --------
<td><img src="/vz/skins/winxp.new/images/1x1.gif" width="10" heigh [...]
<td width="40%">Username</td>
<td align="left" width="60%"><input type="text" name="LoginUser" class="
FlatInput" title="Username" value="mwszgs"></td>
</tr>
<tr>

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

https://50.116.105.215:4643/vz/cp/login-wrapper?LoginUser=mwszgs

Web Application Sitemap — port 4643 / tcp / possible_wls

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313741
Category:	Web Servers
CVE ID:	

THREAT:
The remote web server hosts linkable content that can be crawled by Nessus.

IMPACT:
The remote web server contains linkable content that can be used to gather information about a target.

SOLUTION:

RESULT:

The following sitemap was created from crawling linkable content on the target host :

- https://50.116.105.215:4643/favicon.ico?v=6.0-3215
- https://50.116.105.215:4643/vz/cp
- https://50.116.105.215:4643/vz/cp/login-wrapper
- https://50.116.105.215:4643/vz/skins/winxp.new/common.css?v=6.0-3215
- https://50.116.105.215:4643/vz/skins/winxp.new/plesk.css?v=6.0-3215

Attached is a copy of the sitemap file.

SMTP Server Detection — port 465 / tcp / smtp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	
ID:	8313646
Category:	Service detection
CVE ID:	

THREAT:
An SMTP server is listening on the remote port.

IMPACT:
The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

SOLUTION:
Disable this service if you do not use it, or filter incoming traffic to this port.

RESULT:

Remote SMTP server banner :

220-esc.escgroups.com ESMTP Exim 4.91 #1 Sat, 28 Jul 2018 04:00:46 -0500
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.

Appendices

Hosts Scanned

50.116.105.215

Hosts Not Alive

Option Profile

Scan	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced	
Hosts Discovery:	SYN Standard Scan, UDP Standard Scan
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards. A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host.

An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards. A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host.

Vulnerability Levels

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

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.

MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.