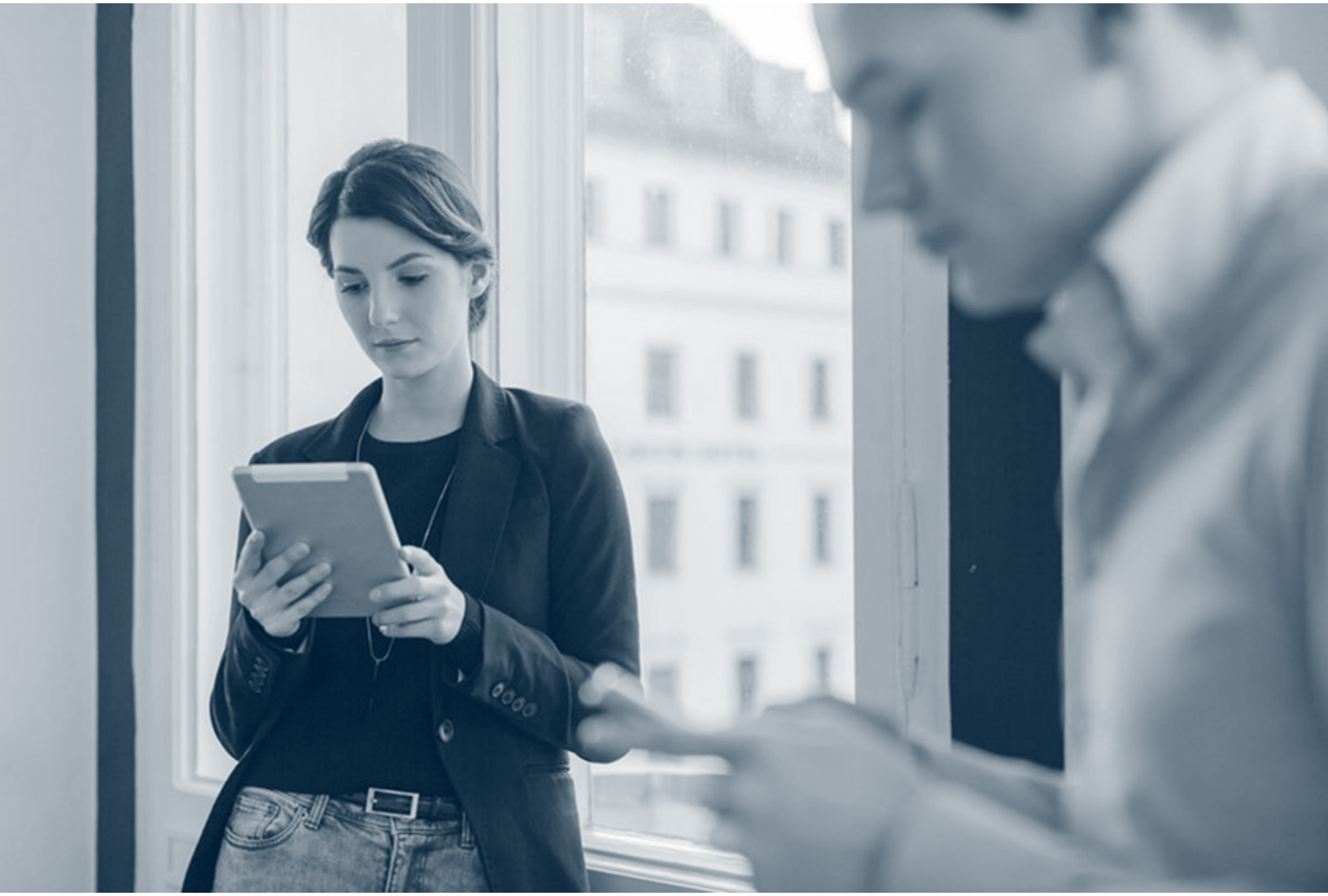
COMMVAULT®

Commvault HyperScale Storage

STIG Certification - Scan Results Detailed



Scan Results Detailed

Note: The RHEL 7 Virtualization Manager plugin with 'Medium' or 'High' risk factors are not applicable, as the virtualization engine is not installed in HyperScale Storage Pool.

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
10107	HTTP Server Type and Version	Web Servers	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: A web server is running on the remote host.					
Description: This plugin attempts to determine the type and the version of the remote web server.					
Solution:					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: Jan 4, 2000 12:00:00 EST					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
10114	ICMP Timestamp Request Remote Date Disclosure	General	Info	172.24.26.73	No
Vulnerability Priority Rating: 3.4					
Synopsis: It is possible to determine the exact time set on the remote host.					
Description: The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.					
Solution: Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score: 0.0					
CVE: CVE-1999-0524					
Patch Publication Date: N/A					
Vuln Publication Date: Jan 1, 1995 12:00:00 EST					
Plugin Publication Date: Aug 1, 1999 12:00:00 EDT					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
10223	RPC portmapper Service Detection	RPC	Info	172.24.26.73	No
Vulnerability Priority Rating: 3.4					
Synopsis: An ONC RPC portmapper is running on the remote host.					
Description: The RPC portmapper is running on this port. The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.					

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score: 0.0

CVE: CVE-1999-0632

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 19, 1999 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
10267	SSH Server Type and Version Information	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: An SSH server is listening on this port.

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

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Oct 12, 1999 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
10287	Traceroute Information	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: It was possible to obtain traceroute information.

Description: Makes a traceroute to the remote host.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Nov 27, 1999 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
10863	SSL Certificate Information	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: This plugin displays the SSL certificate.

Description: This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 19, 2008 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
10881	SSH Protocol Versions Supported	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

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

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

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Mar 6, 2002 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
11111	RPC Services Enumeration	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: An ONC RPC service is running on the remote host.

Description: By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 24, 2002 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
11111	RPC Services Enumeration	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: An ONC RPC service is running on the remote host.

Description: By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 24, 2002 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
11936	OS Identification	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

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

Description: 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:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Dec 9, 2003 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
12053	Host Fully Qualified Domain Name (FQDN) Resolution	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: It was possible to resolve the name of the remote host.

Description: Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Feb 11, 2004 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
12218	mDNS Detection (Remote Network)	Service detection	Medium	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: It is possible to obtain information about the remote host.

Description: The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution: Filter incoming traffic to UDP port 5353, if desired.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Apr 28, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
14272	Netstat Portscanner (SSH)	Port scanners	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Remote open ports can be enumerated via SSH.

Description: Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 15, 2004 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
19506	Nessus Scan Information	Settings	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: This plugin displays information about the Nessus scan.

Description: This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 26, 2005 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
20094	VMware Virtual Machine Detection	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote host is a VMware virtual machine.

Description: According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution: Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Oct 27, 2005 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
21643	SSL Cipher Suites Supported	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service encrypts communications using SSL.

Description: This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jun 5, 2006 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
22869	Software Enumeration (SSH)	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: It was possible to enumerate installed software on the remote host via SSH.

Description: Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, qpkg, dpkg, etc.).

Solution: Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Oct 15, 2006 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
22964	Service Detection	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service could be identified.

Description: 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:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 19, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
22964	Service Detection	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service could be identified.

Description: 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:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 19, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
24260	HyperText Transfer Protocol (HTTP) Information	Web Servers	Info	172.24.26.73	No

Vulnerability Priority Rating:

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

Description: 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:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jan 30, 2007 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25202	Enumerate IPv6 Interfaces via SSH	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description: Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution: Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 11, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25203	Enumerate IPv4 Interfaces via SSH	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description: Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution: Disable any unused IPv4 interfaces.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 11, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25220	TCP/IP Timestamps Supported	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service implements TCP timestamps.

Description: 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:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
25221	Remote listeners enumeration (Linux / AIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description: By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 16, 2007 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
33276	Enumerate MAC Addresses via SSH	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Nessus was able to enumerate MAC addresses on the remote host.

Description: Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution: Disable any unused interfaces.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jun 30, 2008 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
33851	Network daemons not managed by the package system	Misc.	Low	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Some daemon processes on the remote host are associated with programs that have been installed manually.

Description: Some daemon processes on the remote host are associated with programs that have been installed manually.

System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

Solution: Use packages supplied by the operating system vendor whenever possible.

And make sure that manual software installation agrees with your organization's acceptable use and security policies.

Risk Factor: Low

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Aug 8, 2008 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
34098	BIOS Info (SSH)	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: BIOS info could be read.

Description: Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Sep 8, 2008 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
35351	System Information Enumeration (via DMI)	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Information about the remote system's hardware can be read.

Description: Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jan 12, 2009 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
35716	Ethernet Card Manufacturer Detection	Misc.	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The manufacturer can be identified from the Ethernet OUI.

Description: Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Feb 19, 2009 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
39520	Backported Security Patch Detection (SSH)	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Security patches are backported.

Description: Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jun 25, 2009 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
45410	SSL Certificate 'commonName' Mismatch	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description: The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution: If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Apr 3, 2010 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
45432	Processor Information (via DMI)	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Nessus was able to read information about the remote system's processor.

Description: Nessus was able to retrieve information about the remote system's hardware, such as its processor type, by using the SMBIOS (aka DMI) interface.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Apr 6, 2010 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
45433	Memory Information (via DMI)	General	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: Information about the remote system's memory devices can be read.					
Description: Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.					
Solution:					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: Apr 6, 2010 12:00:00 EDT					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
45590	Common Platform Enumeration (CPE)	General	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: It was possible to enumerate CPE names that matched on the remote system.					
Description: 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:					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: Apr 21, 2010 12:00:00 EDT					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
46215	Inconsistent Hostname and IP Address	Settings	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: The remote host's hostname is not consistent with DNS information.					
Description: 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.					
Risk Factor: None					

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 3, 2010 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
50845	OpenSSL Detection	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service appears to use OpenSSL to encrypt traffic.

Description: Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Nov 30, 2010 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
51192	SSL Certificate Cannot Be Trusted	General	Medium	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The SSL certificate for this service cannot be trusted.

Description: The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution: Purchase or generate a proper certificate for this service.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 6.5

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Dec 15, 2010 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
53335	RPC portmapper (TCP)	RPC	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: An ONC RPC portmapper is running on the remote host.

Description: The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Apr 8, 2011 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
54615	Device Type	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

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

Description: 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:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 23, 2011 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
55472	Device Hostname	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: It was possible to determine the remote system hostname.

Description: This plugin reports a device's hostname collected via SSH or WMI.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jun 30, 2011 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
56468	Time of Last System Startup	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The system has been started.

Description: Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Oct 12, 2011 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
56984	SSL / TLS Versions Supported	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service encrypts communications.

Description: This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Dec 1, 2011 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
57582	SSL Self-Signed Certificate	General	Medium	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description: The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in product ion, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution: Purchase or generate a proper certificate for this service.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jan 17, 2012 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
58651	Netstat Active Connections	Misc.	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Active connections are enumerated via the 'netstat' command.

Description: This plugin runs 'netstat' on the remote machine to enumerate all active 'ESTABLISHED' or 'LISTENING' tcp/udp connections.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Apr 10, 2012 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
64582	Netstat Connection Information	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Nessus was able to parse the results of the 'netstat' command on the remote host.

Description: The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Feb 13, 2013 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
66334	Patch Report	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote host is missing several patches.

Description: 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.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jul 8, 2013 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
70544	SSL Cipher Block Chaining Cipher Suites Supported	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description: The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Oct 22, 2013 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
70657	SSH Algorithms and Languages Supported	Misc.	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: An SSH server is listening on this port.

Description: This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Oct 28, 2013 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
70658	SSH Server CBC Mode Ciphers Enabled	Misc.	Low	172.24.26.73	No

Vulnerability Priority Rating: 2.5

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description: The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution: Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encrypt ion.

Risk Factor: Low

STIG Severity:

CVSS V3 Base Score:

CVE: CVE-2008-5161

Patch Publication Date: N/A

Vuln Publication Date: Nov 24, 2008 12:00:00 EST

Plugin Publication Date: Oct 28, 2013 12:00:00 EDT

Exploit Ease: No known exploits are available

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
83303	Unix / Linux - Local Users Information : Passwords Never Expire	Misc.	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: At least one local user has a password that never expires.

Description: Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

Solution: Allow or require users to change their passwords regularly.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 10, 2015 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
84502	HSTS Missing From HTTPS Server	Web Servers	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote web server is not enforcing HSTS.

Description: The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution: Configure the remote web server to use HSTS.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jul 2, 2015 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
86420	Ethernet MAC Addresses	General	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: This plugin gathers MAC addresses from various sources and consolidates them into a list.					
Description: This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.					
Solution:					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: Oct 16, 2015 12:00:00 EDT					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
90707	SSH SCP Protocol Detection	Misc.	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: The remote host supports the SCP protocol over SSH.					
Description: The remote host supports the Secure Copy (SCP) protocol over SSH.					
Solution:					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: Apr 26, 2016 12:00:00 EDT					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
95928	Linux User List Enumeration	General	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: Nessus was able to enumerate local users and groups on the remote host.					
Description: Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote host.					
Solution: None					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: Dec 19, 2016 12:00:00 EST					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)	Misc.	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: Information about the remote host can be disclosed via an authenticated session.					
Description: Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.					
Solution:					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: May 30, 2017 12:00:00 EDT					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
104743	TLS Version 1.0 Protocol Detection	Service detection	Info	172.24.26.73	No
Vulnerability Priority Rating:					
Synopsis: The remote service encrypts traffic using an older version of TLS.					
Description: The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.					
Solution: Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.					
Risk Factor: None					
STIG Severity:					
CVSS V3 Base Score:					
CVE:					
Patch Publication Date: N/A					
Vuln Publication Date: N/A					
Plugin Publication Date: Nov 22, 2017 12:00:00 EST					
Exploit Ease:					

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
104774	RHEL 7 : .NET Core (RHSA-2017:3248	Red Hat Local Security Checks	Medium	172.24.26.73	No
Vulnerability Priority Rating: 3.6					
Synopsis: The remote Red Hat host is missing one or more security updates.					
Description: A security update for .NET Core on RHEL is now available. Red Hat Product Security has rated this update as having a security impact of Low. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link (s) in the References section.					

New versions of .NET Core that address several security vulnerabilities are now available. The updated versions are .NET Core 1.0.8, 1.1.5 and 2.0.3.

Security Fix(es) :

* By providing an invalid culture, an attacker can cause a recursive lookup that leads to a denial of service when running on certain Windows platforms. (CVE-2017-8585)

* Supplying a specially crafted certificate can cause an infinite X509Chain, resulting in a denial of service. (CVE-2017-11770)

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.5

CVE: CVE-2017-11770,CVE-2017-8585

Patch Publication Date: Nov 20, 2017 12:00:00 EST

Vuln Publication Date: Jul 11, 2017 12:00:00 EDT

Plugin Publication Date: Nov 27, 2017 12:00:00 EST

Exploit Ease: No known exploits are available

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
107114	RHEL 7 : .NET Core on Red Hat Enterprise Linux (RHSA-2018:0379	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 3.6

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for rh-dotnet20-dotnet, rh-dotnetcore10-dotnetcore, and rh-dotnetcore11-dotnetcore is now available for .NET Core on Red Hat Enterprise Linux.

Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

.NET Core is a managed software framework. It implements a subset of the .NET framework APIs and includes a CLR implementation.

New versions of .NET Core that address several security vulnerabilities are now available. The updated versions are .NET Core 1.0.9, 1.1.6, and 2.0.5.

Security Fix(es) :

* .NET Core: Improper processing of XML documents can cause a denial of service (CVE-2018-0764)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.5

CVE: CVE-2018-0764

Patch Publication Date: Mar 1, 2018 12:00:00 EST

Vuln Publication Date: Jan 10, 2018 12:00:00 EST

Plugin Publication Date: Mar 2, 2018 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
108395	RHEL 7 : .NET Core on Red Hat Enterprise Linux (RHSA-2018:0522	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 3.6

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: Updates for rh-dotnet20-dotnet, rh-dotnetcore10-dotnetcore, and rh-dotnetcore11-dotnetcore are now available for .NET Core on Red Hat Enterprise Linux.

Red Hat Product Security has rated this update as having a security impact of Low. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link (s) in the References section.

.NET Core is a managed software framework. It implements a subset of the .NET framework APIs and includes a CLR implementation.

New versions of .NET Core that address several security vulnerabilities are now available. The updated versions are .NET Core 1.0.10, 1.1.7, and 2.0.6.

These correspond to the March 2018 security release by .NET Core upstream projects.

Security Fix(es) :

* .NET Core: Hash Collision Denial of Service (CVE-2018-0875)

Red Hat would like to thank Ben Adams (Illyriad Games) for reporting this issue.

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.5

CVE: CVE-2018-0875

Patch Publication Date: Mar 14, 2018 12:00:00 EDT

Vuln Publication Date: Mar 14, 2018 12:00:00 EDT

Plugin Publication Date: Mar 16, 2018 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
108996	RHEL 7 : pcs (RHSA-2018:1060	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 3.6

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for pcs is now available for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The pcs packages provide a command-line configuration system for the Pacemaker and Corosync utilities.

Security Fix(es) :

* pcs: Privilege escalation via authorized user malicious REST call (CVE-2018-1079)

* pcs: Debug parameter removal bypass, allowing information disclosure (CVE-2018-1086)

* rack-protection: Timing attack in authenticity_token.rb (CVE-2018-1000119)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

The CVE-2018-1079 issue was discovered by Ondrej Mular (Red Hat) and the CVE-2018-1086 issue was discovered by Cedric Buissart (Red Hat).

Solution: Update the affected pcs, pcs-debuginfo and / or pcs-snmp packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.5

CVE: CVE-2018-1000119,CVE-2018-1079,CVE-2018-1086

Patch Publication Date: Apr 10, 2018 12:00:00 EDT

Vuln Publication Date: Mar 7, 2018 12:00:00 EST

Plugin Publication Date: Apr 11, 2018 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
110095	Authentication Success	Settings	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description: Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, no access or privilege issues were reported, and no subsequent failures were reported for the successful credentials.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: May 24, 2018 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
110483	Unix / Linux Running Processes Information	General	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description: Generated report details the running processes on the target machine at scan time.
This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jun 12, 2018 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
111031	RHEL 7 : .NET Core on Red Hat Enterprise Linux (RHSA-2018:2167	Red Hat Local Security Checks	Low	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: Updates for rh-dotnet20-dotnet, rh-dotnet21-dotnet, rh-dotnetcore10-dotnetcore, and rh-dotnetcore11-dotnetcore are now available for .NET Core on Red Hat Enterprise Linux.

Red Hat Product Security has rated this update as having a security impact of Low.

.NET Core is a managed software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation.

New versions of .NET Core that address several security vulnerabilities are now available. The updated versions are .NET Core 1.0.12, 1.1.9, 2.0.9, and 2.1.2.

These versions correspond to the July 2018 security release by .NET Core upstream projects.

Security Fix(es) :

Default inclusions for applications built with .NET Core have been updated to reference the newest versions and their security fixes.

For more information, please refer to the upstream docs :

* .NET Core 1.0.12: https://github.com/dotnet/core/issues/1768

* .NET Core 1.1.9: https://github.com/dotnet/core/issues/1767

* .NET Core 2.0.9: https://github.com/dotnet/core/issues/1766

* .NET Core 2.1.2: https://github.com/dotnet/core/issues/1765

Solution: Update the affected packages.

Risk Factor: Low

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: Jul 11, 2018 12:00:00 EDT

Vuln Publication Date: Jul 11, 2018 12:00:00 EDT

Plugin Publication Date: Jul 12, 2018 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
117887	Local Checks Enabled	Settings	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Nessus was able to log in to the remote host using the provided credentials and enable local checks.

Description: Nessus was able to enable local checks because it was possible to log in to the remote host using provided credentials, the remote host was identified as an operating system or device for which local checks are available, and the necessary information was able to be obtained from the remote host in order to enable local checks.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Oct 2, 2018 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
118127	RHEL 7 : dotNET (RHSA-2018:2902	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 3.6

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: Updates for rh-dotnetcore11-dotnetcore, and rh-dotnetcore10-dotnetcore are now available for .NET Core on Red Hat Enterprise Linux.

Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

.NET Core is a managed software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation.

New versions of .NET Core that address several security vulnerabilities are now available. The updated versions are .NET Core 1.1.1 and 1.0.13.

These versions correspond to the October 2018 security release by .NET Core upstream projects.

Security Fix(es) :

* An information disclosure vulnerability exists in .NET Core when authentication information is inadvertently exposed in a redirect (CVE-2018-8292)

For more information, please refer to the upstream docs in the References section.

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.5

CVE: CVE-2018-8292

Patch Publication Date: Oct 9, 2018 12:00:00 EDT

Vuln Publication Date: Oct 10, 2018 12:00:00 EDT

Plugin Publication Date: Oct 16, 2018 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
119602	Python Flask Installed (Linux)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Python Flask is installed on the remote host.

Description: Flask, a micro web framework written in Python, is installed on the remote Linux host.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Dec 12, 2018 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
119778	Flask < 0.12.3 Denial of Service Vulnerability	CGI abuses	Medium	172.24.26.73	No

Vulnerability Priority Rating: 3.6

Synopsis: A web development framework on the remote host is affected by a denial of service vulnerability.

Description: The version of Pallets Flask on the remote host is prior to 0.12.3. It is, therefore, affected by a denial of service vulnerability in the JSON decoding process due to improper input validation. An unauthenticated attacker can exploit this issue by providing JSON data in a non-text related encoding, which could result in unexpected memory use.

Solution: Upgrade to Flask version 0.12.3 or later.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.5

CVE: CVE-2018-1000656

Patch Publication Date: Apr 26, 2018 12:00:00 EDT

Vuln Publication Date: Apr 26, 2018 12:00:00 EDT

Plugin Publication Date: Dec 19, 2018 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
121010	TLS Version 1.1 Protocol Detection	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: The remote service encrypts traffic using an older version of TLS.

Description: The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

PCI DSS v3.2 still allows TLS 1.1 as of June 30, 2018, but strongly recommends the use of TLS 1.2. A proposal is currently before the IETF to fully deprecate TLS 1.1 and many vendors have already proactively done this.

Solution: Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Jan 8, 2019 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
121575	Ansible Installed (Linux/UNIX)	Service detection	Info	172.24.26.73	No

Vulnerability Priority Rating:

Synopsis: Ansible is installed on this host.

Description: Ansible, an IT automation and management application, was found on the remote host.

Solution:

Risk Factor: None

STIG Severity:

CVSS V3 Base Score:

CVE:

Patch Publication Date: N/A

Vuln Publication Date: N/A

Plugin Publication Date: Feb 4, 2019 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
122330	RHEL 7 : dotNET (RHSA-2019:0349	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 3.6

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: Updates for rh-dotnetcore10-dotnetcore, rh-dotnetcore11-dotnetcore, rh-dotnet21-dotnet, and rh-dotnet22-dotnet are now available for .NET Core on Red Hat Enterprise Linux.

Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

.NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation.

New versions of .NET Core that address security vulnerabilities are now available. The updated versions are .NET Core 1.0.14, 1.1.11, 2.1.8, and 2.2.2.

Security Fix(es) :

* .dotnet: Domain-spoofing attack in System.Uri (CVE-2019-0657)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

For more information, please refer to the upstream doc in the References section.

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 5.9

CVE: CVE-2019-0657

Patch Publication Date: Feb 14, 2019 12:00:00 EST

Vuln Publication Date: Mar 5, 2019 12:00:00 EST

Plugin Publication Date: Feb 20, 2019 12:00:00 EST

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
122886	RHEL 7 : dotNET (RHSA-2019:0544	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 3.6

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: Updates for rh-dotnetcore10-dotnetcore, rh-dotnetcore11-dotnetcore, rh-dotnet21-dotnet, and rh-dotnet22-dotnet are now available for .NET Core on Red Hat Enterprise Linux.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

.NET Core is a managed-software framework. It implements the .NET standard APIs and several additional APIs, and it includes a CLR implementation.

New versions of .NET Core that address security vulnerabilities are now available. The updated versions are .NET Core 1.0.15, 1.1.12, 2.1.9, and 2.2.3.

Security Fix(es) :

* A tampering vulnerability exists in NuGet software when executed in a Linux or Mac environment. (CVE-2019-0757)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

For more information, please refer to the upstream doc in the References section.

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 6.5

CVE: CVE-2019-0757

Patch Publication Date: Mar 13, 2019 12:00:00 EDT

Vuln Publication Date: Apr 9, 2019 12:00:00 EDT

Plugin Publication Date: Mar 18, 2019 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
125045	RHEL 7 : Virtualization Manager (RHSA-2019:1179) (MDSUM/RIDL) (MFBDS/RIDL/ ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 8.5

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for qemu-kvm-rhev is now available for Red Hat Virtualization 4 for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on a variety of architectures. The qemu-kvm-rhev packages provide the user-space component for running virtual machines that use KVM in environments managed by Red Hat products.

Security Fix(es) :

* A flaw was found in the implementation of the 'fill buffer', a mechanism used by modern CPUs when a cache-miss is made on L1 CPU cache. If an attacker can generate a load operation that would create a page fault, the execution will continue speculatively with incorrect data from the fill buffer while the data is fetched from higher level caches. This response time can be measured to infer data in the fill buffer. (CVE-2018-12130)

* Modern Intel microprocessors implement hardware-level micro-optimizations to improve the performance of writing data back to CPU caches. The write operation is split into STA (STore Address) and STD (STore Data) sub-operations. These sub-operations allow the processor to hand-off address generation logic into these sub-operations for optimized writes. Both of these sub-operations write to a shared distributed processor structure called the 'processor store buffer'. As a result, an unprivileged attacker could use this flaw to read private data resident within the CPU's processor store buffer. (CVE-2018-12126)

* Microprocessors use a 'load port' subcomponent to perform load operations from memory or IO. During a load operation, the load port receives data from the memory or IO subsystem and then provides the data to the CPU registers and operations in the CPU's pipelines.
Stale load operations results are stored in the 'load port' table until overwritten by newer operations. Certain load-port operations triggered by an attacker can be used to reveal data about previous stale requests leaking data back to the attacker via a timing side-channel. (CVE-2018-12127)

* Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
(CVE-2019-11091)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity: I

CVSS V3 Base Score: 6.5

CVE: CVE-2018-12126,CVE-2018-12127,CVE-2018-12130,CVE-2019-11091

Patch Publication Date: May 14, 2019 12:00:00 EDT

Vuln Publication Date: May 30, 2019 12:00:00 EDT

Plugin Publication Date: May 14, 2019 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
125322	RHEL 7 : dotNET (RHSA-2019:1236	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 4.4

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: Updates for rh-dotnetcore10-dotnetcore, rh-dotnetcore11-dotnetcore, rh-dotnet21-dotnet, rh-dotnet22-dotnet and rh-dotnet22-curl are now available for .NET Core on Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

.NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation.

New versions of .NET Core that address security vulnerabilities are now available. The updated versions are .NET Core 1.0.16, 1.1.13, 2.1.11, and 2.2.5.

Security Fix(es) :

* dotNET: timeouts for regular expressions are not enforced (CVE-2019-0820)

* dotNET: infinite loop in URI.TryCreate leading to ASP.Net Core Denial of Service (CVE-2019-0980)

* dotNET: crash in IPAddress.TryCreate leading to ASP.Net Core Denial of Service (CVE-2019-0981)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Bug Fix(es) :

* Re-enable bash completion in rh-dotnet22-dotnet (BZ#1654863)

* Error rebuilding rh-dotnet22-curl in CentOS (BZ#1678932)

* Broken apphost caused by unset DOTNET_ROOT (BZ#1703479)

* Make bash completion compatible with rh-dotnet22 packages (BZ#1705259)

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.5

CVE: CVE-2019-0820,CVE-2019-0980,CVE-2019-0981

Patch Publication Date: May 15, 2019 12:00:00 EDT

Vuln Publication Date: May 16, 2019 12:00:00 EDT

Plugin Publication Date: May 22, 2019 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
125445	RHEL 7 : pacemaker (RHSA-2019:1278	Red Hat Local Security Checks	Medium	172.24.26.73	No

Vulnerability Priority Rating: 6.7

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for pacemaker is now available for Red Hat Enterprise Linux 7.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

The Pacemaker cluster resource manager is a collection of technologies working together to maintain data integrity and application availability in the event of failures.

Security Fix(es) :

* pacemaker: Insufficient local IPC client-server authentication on the client's side can lead to local privesc (CVE-2018-16877)

* pacemaker: Insufficient verification inflicted preference of uncontrolled processes can lead to DoS (CVE-2018-16878)

* pacemaker: Information disclosure through use-after-free (CVE-2019-3885)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Solution: Update the affected packages.

Risk Factor: Medium

STIG Severity:

CVSS V3 Base Score: 7.8

CVE: CVE-2018-16877,CVE-2018-16878,CVE-2019-3885

Patch Publication Date: May 27, 2019 12:00:00 EDT

Vuln Publication Date: Apr 18, 2019 12:00:00 EDT

Plugin Publication Date: May 28, 2019 12:00:00 EDT

Exploit Ease:

Plugin	Plugin Name	Family	Severity	IP Address	Exploit?
127640	RHEL 7 : Virtualization Manager (RHSA-2019:1968	Red Hat Local Security Checks	High	172.24.26.73	No

Vulnerability Priority Rating: 7.4

Synopsis: The remote Red Hat host is missing one or more security updates.

Description: An update for qemu-kvm-rhev is now available for Red Hat Virtualization for Red Hat Virtualization Host 7.

Red Hat Product Security has rated this update as having a Important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link (s) in the References section.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on a variety of architectures. The qemu-kvm-rhev packages provide the user-space component for running virtual machines that use KVM in environments managed by Red Hat products.

Security Fix(es) :

* CVE-2018-20815 QEMU: device_tree: heap buffer overflow while loading device tree blob

* CVE-2019-6778 QEMU: slirp: heap buffer overflow in tcp_em

This update fixes the following bug :

* 1705364 RHV VM pauses when 'dd' issued inside guest to a direct lun configured as virtio-scsi with scsi-passthrough

Users of qemu-kvm are advised to upgrade to these updated packages.
After installing this update, shut down all running virtual machines.
Once all virtual machines have shut down, start them again for this update to take effect.

Solution: Update the affected packages.

Risk Factor: High

STIG Severity:

CVSS V3 Base Score: 9.8
CVE: CVE-2018-20815,CVE-2019-6778
Patch Publication Date: Jul 30, 2019 12:00:00 EDT
Vuln Publication Date: Mar 21, 2019 12:00:00 EDT
Plugin Publication Date: Aug 12, 2019 12:00:00 EDT
Exploit Ease:

Tenable's algorithms factor in data from a variety of sources including Tenable proprietary research, machine based learning, and leading third party intelligence including, but not limited to, Recorded Future.

Visit the Commvault Documentation website for complete documentation of Commvault products.