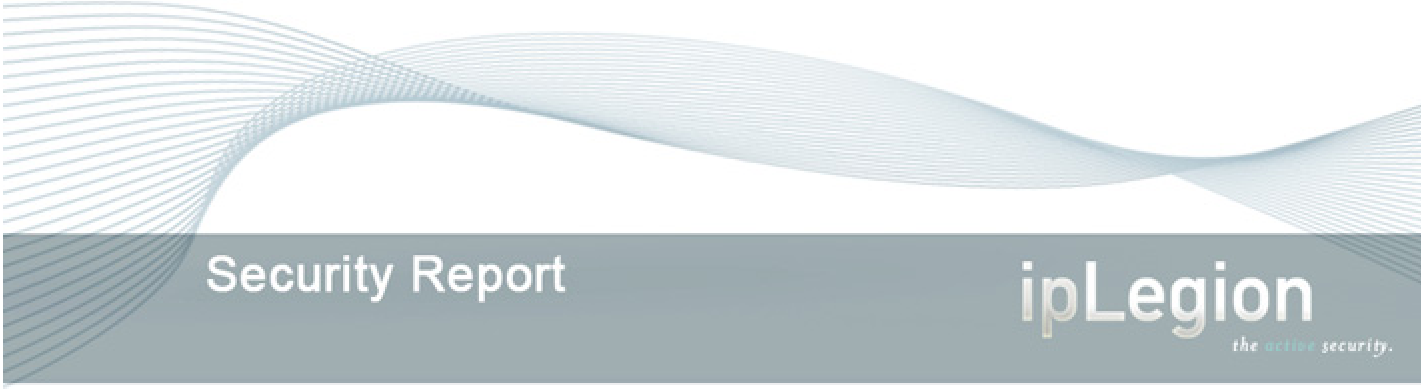
eMaze
informed security

Activity Report

This report includes important security information about your current network status.
Start Scan: lun, 27 ott 2008 14:57:48 +0100
Campaign Name: Scansione rapida
Activity Id: 4460



Activity summary

Activity Id:	4460		
User:	ipLegion Administrator admin@emaze.net	Supervisor:	-
Campaign Name:	Scansione rapida	Status:	Completed
Start Scan:	lun, 27 ott 2008 14:57:48 +0100	Duration:	00h:31m:54s
Settings:	Preferenze per la scansione rapida		
Targets:	10.4.10.37/32		

10.4.10.37

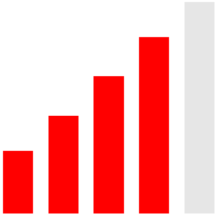
Host Summary

Operating System:	Linux	MAC Address:	00:0C:29:5F:C0:C0
Hostname:	-		

Exposure Level

HIGH

47



Vulnerability Level	47/100
Bruteforced Accounts	Not Executed
Local Vulnerability Level	Not Executed

Scouts

Scout:	Scout Rete Test (3)

Run Modules

Name	Time Begin	Time End
Network Discovery	lun, 27 ott 2008 14:57:48 +0100	lun, 27 ott 2008 14:57:48 +0100
Vulnerability Assessment	lun, 27 ott 2008 14:57:48 +0100	lun, 27 ott 2008 15:29:39 +0100

Vulnerability Assessment Module Results

Vulnerability Level: **47 / 100**

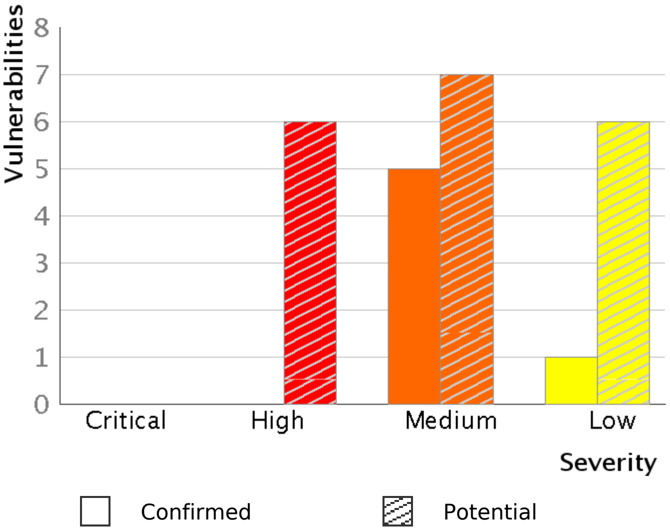
Vulnerability Assessment Summary

Start Scan:	lun, 27 ott 2008 14:57:48 +0100	Stop Scan:	lun, 27 ott 2008 15:29:39 +0100

Vulnerabilities Found

Vulnerabilities Found

Severity	Confirmed	Potential
Critical:	0	0
High:	0	6
Medium:	5	7
Low:	1	6
Total:	**6**	**19**



Trend Analysis

No previous scan data available.

Confirmed Vulnerabilities by Family

Vulnerability Type	Critical	High	Medium	Low	Info
CLIENT SIDE					1
DNS SERVERS					1
FTP SERVER			1		1
MISCELLANEOUS SERVER			3		8
NETBIOS SERVICES					1
NETWORK STACK					1
REMOTE ADMINISTRATION			1		3
UNIX RPC				1	7
Total	**0**	**0**	**5**	**1**	**23**

Open Ports

Protocol	Port	Service
TCP		

Open Ports

Protocol	Port	Service
	21	ftp
	22	ssh
	53	domain
	80	tcpwrapped
	111	rpcbind
	139	tcpwrapped
	443	tcpwrapped
	838	rquotad
	1024	status
	1025	sgi_fam
	1026	mountd
UDP		
	53	domain
	111	rpcbind
	137	netbios-ns
	138	netbios-dgm
	835	rquotad
	1024	status
	1026	nlockmgr
	1027	mountd
	2049	nfs

Confirmed Vulnerabilities by Severity

Severity	Vulnerability	Port	Status
Medium	Anonymous FTP Server	21/TCP	New
Medium	SSH Protocol Version 1 Enabled	22/TCP	New
Medium	SSL Certificate Expired	443/TCP	New
Medium	SSL Self Signed Certificate	443/TCP	New
Medium	SSLv2 Support Enabled	443/TCP	New
Low	RPC nlockmgr Service allows proxying of NFS requests	1026/UDP	New
Info	DNS Server Running	53/UDP	New
Info	FTP Server Running	21/TCP	New
Info	NFS Server Running	2049/UDP	New

Confirmed Vulnerabilities by Severity

Severity	Vulnerability	Port	Status
Info	NetBIOS Name Service Running	137/UDP	New
Info	Portmap Daemon Running	111/UDP	New
Info	Portmap Daemon Running	111/TCP	New
Info	RPC nlockmgr Service Running	1026/UDP	New
Info	RPC rquotad Service Running	835/UDP	New
Info	RPC rquotad Service Running	838/TCP	New
Info	RPC status Service Running	1024/UDP	New
Info	RPC status Service Running	1024/TCP	New
Info	Response to ICMP packets	-	New
Info	Response with ICMP Port Unreachable to closed ports	-	New
Info	SSH Server Running	22/TCP	New
Info	SSH Supported Algorithms	22/TCP	New
Info	SSHv2 Key Fingerprint	22/TCP	New
Info	SSL Certificate Information	443/TCP	New
Info	SSL Supported Ciphers List	443/TCP	New
Info	SSL Supported Protocols	443/TCP	New
Info	Software Installed	-	New
Info	UNIX RPC Services	111/UDP	New
Info	UNIX RPC Services	111/TCP	New
Info	VMWare Virtual Machine Running	-	New

The status field is a synthesis of any change that may have occurred between the current and the previous activity of the same campaign. Possible values are: ***New****, if the vulnerability wasn't found in the previous activity and was found in the current one.* ***Already known****, if the vulnerability was found both in the previous and in the current activity.* ***Removed****, if the vulnerability found in the previous activity wasn't found in the current one.* ***Port closed****, if the appliance, for some reason, couldn't check in the current activity for a vulnerability that was found in the previous one.*

Confirmed Vulnerabilities by Port

Protocol	Port	Service	Vulnerability
TCP			
	21	ftp	Anonymous FTP Server
	21	ftp	FTP Server Running
	22	ssh	SSH Protocol Version 1 Enabled
	22	ssh	SSH Server Running
	22	ssh	SSH Supported Algorithms
	22	ssh	SSHv2 Key Fingerprint

Confirmed Vulnerabilities by Port

Protocol	Port	Service	Vulnerability
	111	rpcbind	Portmap Daemon Running
	111	rpcbind	UNIX RPC Services
	443	tcpwrapped	SSL Certificate Expired
	443	tcpwrapped	SSL Certificate Information
	443	tcpwrapped	SSL Self Signed Certificate
	443	tcpwrapped	SSL Supported Ciphers List
	443	tcpwrapped	SSL Supported Protocols
	443	tcpwrapped	SSLv2 Support Enabled
	838	rquotad	RPC rquotad Service Running
	1024	status	RPC status Service Running
UDP			
	53	domain	DNS Server Running
	111	rpcbind	Portmap Daemon Running
	111	rpcbind	UNIX RPC Services
	137	netbios-ns	NetBIOS Name Service Running
	835	rquotad	RPC rquotad Service Running
	1024	status	RPC status Service Running
	1026	nlockmgr	RPC nlockmgr Service Running
	1026	nlockmgr	RPC nlockmgr Service allows proxying of NFS requests
	2049	nfs	NFS Server Running

Confirmed Vulnerabilities Details

🟧🟧🟧⬜⬜ Anonymous FTP Server

Emaze ID	10064
Severity	Medium
Service	21 / TCP (ftp)
Family	FTP SERVER
Published	1-gen-2005
Description	The FTP server host allows connections from an anonymous user. A remote attacker could exploit this flaw to download files hosted on the FTP server.
Fix	It is strongly recommended to disable anonymous access to the FTP server.
Standards	CVE: 1999-0497 CVSS: 0.0
Details	Anonymous Login: Credentials:

Confirmed Vulnerabilities Details

```
        Password: anonymous@
        User: anonymous

Root Path: /
File List: drwxr-xr-x    2 0        0           4096 Feb 28  2003 pub
```

■■■□□ SSH Protocol Version 1 Enabled

Emaze ID	10009
Severity	Medium
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	31-dic-2004
Description	The remote host has SSH (Secure Shell) protocol version 1 enabled. A remote attacker could use this configuration error to perform successfully man-in-the-middle attacks.
Fix	It is recommended to disable the service if not used or to disable version 1 in favor of SSH protocol version 2.
Standards	CVE: 2001-0361 CVSS: 6.4 XForce: 6082

■■■□□ SSL Certificate Expired

Emaze ID	10100
Severity	Medium
Service	🔒 443 / TCP (tcpwrappeds)
Family	MISCELLANEOUS SERVER
Published	1-gen-2006
Description	The remote host has SSL Certificate expired
Fix	It is recommended to disable the service if not used.
Standards	CVE: 2001-1008 CVSS: 7.5 XForce: 7048

■■■□□ SSL Self Signed Certificate

Emaze ID	10101
Severity	Medium
Service	🔒 443 / TCP (tcpwrappeds)
Family	MISCELLANEOUS SERVER
Published	1-gen-2006
Description	The Secure Socket Layer (SSL) protocol allows secure communication between client and server. A SSL session between server and client is established using certificates. It is possible that the server certificate is self signed. As a consequence a potential client is not able to verify the server identity through a Public Key Infrastructure.
Fix	It is recommended to sign certificates using a public trusted Certification Authority. See the link below for a list of third party Certification Authorities: http://www.dmoz.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/
Standards	CVE: 2004-0590 CVSS: 10.0

Confirmed Vulnerabilities Details

XForce: 16515

🟧🟧🟧⬜⬜ SSLv2 Support Enabled

Emaze ID	10068
Severity	Medium
Service	🔒 443 / TCP (tcpwrappeds)
Family	MISCELLANEOUS SERVER
Published	1-gen-2005
Description	The Secure Socket Layer (SSL) protocol allows secure communication between a client and a server. The remote host allows to negotiate SSL connection using SSL protocol version 2. This protocol is known to have multiple cryptography flaws that could allow a remote attacker to decrypt SSL connections or maliciously modify messages. All cryptography flaws have been fixed in SSLv3 (or TLSv1). Notice that SSLv2 is enabled by default for backward compatibility.
Fix	It is recommended to disable SSLv2 in favor of SSLv3 or TLSv1. The following link provides more information on how to enable SSLv3 or TLSv1 for the Apache HTTP Server: http://httpd.apache.org/docs/2.0/mod/mod_ssl.html The following link provides more information on how to enable SSLv3 or TLSv1 for the Microsoft IIS: http://support.microsoft.com/kb/245030
Reference	http://www.schneier.com/paper-ssl.pdf

🟨🟨⬜⬜⬜ RPC nlockmgr Service allows proxying of NFS requests

Emaze ID	10186
Severity	Low
Service	1026 / UDP (nlockmgr)
Family	UNIX RPC
Published	1-gen-2006
Description	RPC nlockmgr service allows proxying of NFS requests which means that even if an authorized user blocked NFS traffic on your network, a malicious user can perform NFS queries through the nlockmgr service bypassing your restriction.
Fix	It is recommended to disable the service if not used or allow access only to trusted host/networks.
Standards	CVE: 2000-0508

🟦⬜⬜⬜⬜ DNS Server Running

Emaze ID	10043
Severity	Info
Service	53 / UDP (domain)
Family	DNS SERVERS
Published	1-gen-2005
Description	The Domain Name System or DNS is a system that stores information about hostnames and domain names in a kind of distributed database on networks, such as the Internet. Most importantly, it provides a physical location (IP address) for each hostname, and lists the mail exchange servers accepting e-mail for each domain.
Fix	It is recommended to disable the service if not used.
Standards	CVE: 1999-0622
Details	Detected BIND version 9.2.1

🟦⬜⬜⬜⬜ FTP Server Running

Emaze ID	10006

Confirmed Vulnerabilities Details

Severity	Info
Service	21 / TCP (ftp)
Family	FTP SERVER
Published	31-dic-2004
Description	The remote host is running a FTP (File Transfer Protocol) service. FTP is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. There are two hosts involved in an FTP transfer: a server and a client. The FTP server, running FTP server software, listens on the network for connection requests from other hosts. The client computer, running FTP client software, initiates a connection to the server.
Fix	It is recommended to filter connections to the FTP server from untrusted hosts or disable the service if not used.
Standards	CVE: 1999-0614
Details	220 (vsFTPd 1.1.3)

🟦⬜⬜⬜⬜ NFS Server Running

Emaze ID	10121
Severity	Info
Service	2049 / UDP (nfs)
Family	MISCELLANEOUS SERVER
Published	1-gen-2006
Description	The remote host is running a NFS (Network File System) server. NFS is a protocol defined as a distributed file system which allows a computer to access files over a network as easily as if they were on its local disks.
Fix	It is recommended to disable the service if not used or allow access only to trusted host/networks.
Standards	CVE: 1999-0631

🟦⬜⬜⬜⬜ NetBIOS Name Service Running

Emaze ID	10120
Severity	Info
Service	137 / UDP (netbios-ns)
Family	NETBIOS SERVICES
Published	1-gen-2006
Description	Network Basic Input/Output System (NetBIOS) is a protocol that allows applications on separate hosts to communicate over a local area network. At each station it is possible to assign multiple names.
Fix	It is recommended to filter incoming connections on this port.
Standards	CVE: 1999-0621
Details	NetBIOS nodes: MYGROUP: Workgroup / Domain name (0X0) Master Browser (0X1D) Browser Service Elections (0X1E) RH90: Computer name (0X0) Messenger Service (0X3) File Server Service (0X20) NetBIOS name: RH90

Confirmed Vulnerabilities Details

Portmap Daemon Running

Emaze ID	10037
Severity	Info
Service	111 / UDP (rpcbind)
Family	MISCELLANEOUS SERVER
Published	1-gen-2005
Description	The Portmap Daemon converts RPC program numbers into Internet port numbers. When an RPC server starts up, it registers with the portmap daemon. The server tells the daemon which port number it is listening to and which RPC program numbers it serves. Thus, the portmap daemon knows the location of every registered port on the host and which programs are available on each of these ports.
Fix	It is recommended to disable the service if not used.
Standards	CVE: 1999-0632 CVSS: 0.0

Portmap Daemon Running

Emaze ID	10037
Severity	Info
Service	111 / TCP (rpcbind)
Family	MISCELLANEOUS SERVER
Published	1-gen-2005
Description	The Portmap Daemon converts RPC program numbers into Internet port numbers. When an RPC server starts up, it registers with the portmap daemon. The server tells the daemon which port number it is listening to and which RPC program numbers it serves. Thus, the portmap daemon knows the location of every registered port on the host and which programs are available on each of these ports.
Fix	It is recommended to disable the service if not used.
Standards	CVE: 1999-0632 CVSS: 0.0

RPC nlockmgr Service Running

Emaze ID	10170
Severity	Info
Service	1026 / UDP (nlockmgr)
Family	UNIX RPC
Published	1-gen-2006
Description	nlockmgr RCP service is used by NFS (Network File System) to allow NFS clients to perform file locking.
Fix	It is recommended to disable the service if not used.

RPC rquotad Service Running

Emaze ID	10166
Severity	Info
Service	835 / UDP (rquotad)
Family	UNIX RPC
Published	1-gen-2006

Confirmed Vulnerabilities Details

Description	rquotad RPC service returns quotas for a user of a local file system which is mounted by a remote machine over the NFS.
Fix	It is recommended to disable the service if not used.
Standards	CVE: 1999-0625 CVSS: 0.0

RPC rquotad Service Running

Emaze ID	10166
Severity	Info
Service	838 / TCP (rquotad)
Family	UNIX RPC
Published	1-gen-2006
Description	rquotad RPC service returns quotas for a user of a local file system which is mounted by a remote machine over the NFS.
Fix	It is recommended to disable the service if not used.
Standards	CVE: 1999-0625 CVSS: 0.0

RPC status Service Running

Emaze ID	10036
Severity	Info
Service	1024 / UDP (status)
Family	UNIX RPC
Published	1-gen-2005
Description	The RPC status allows an attacker to know the current state of certain RPC operation calls.
Fix	It is recommended to disable the service if not used or allow access only to trusted host/networks.

RPC status Service Running

Emaze ID	10036
Severity	Info
Service	1024 / TCP (status)
Family	UNIX RPC
Published	1-gen-2005
Description	The RPC status allows an attacker to know the current state of certain RPC operation calls.
Fix	It is recommended to disable the service if not used or allow access only to trusted host/networks.

Response to ICMP packets

Emaze ID	10049
Severity	Info
Family	MISCELLANEOUS SERVER
Published	1-gen-2005
Description	ICMP is used by the transport layer to send one-way information messages to a remote host. An attacker may inject packets into the network causing remote host Denial of Service conditions. Typical ICMP attacks are: ICMP DOS attack, ICMP Smurf, Ping of death, ICMP PING flooding and ICMP nuke attack.
Fix	It is recommended to filter ICMP packets using firewalling techniques.

Confirmed Vulnerabilities Details

Details	Transmit Timestamp: 0 days 14 hours 10 minutes 30 seconds after midnight UTC; Response: 51030316 Echo Request: 100% Originate Timestamp: Mon Oct 27 15:57:03 2008; Response: 1225119423 Information Request: 0% Network Mask Request: 0% Receive Timestamp: 0 days 14 hours 10 minutes 30 seconds after midnight UTC; Response: 51030316 Timestamp Request: 100%

■□□□□ Response with ICMP Port Unreachable to closed ports

Emaze ID	10716
Severity	Info
Family	NETWORK STACK
Published	1-gen-2008
Description	Iplegion checked if the remote machine replies with an ICMP Port Unreachable packet when opening a socket with a closed port. This is a normal behaviour that sometimes changes because of firewalls ruleset.
Details	Port Unreachable: True

■□□□□ SSH Server Running

Emaze ID	10007
Severity	Info
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	31-dic-2004
Description	The remote host is running a SSH (Secure Shell) server. SSH is a network protocol that allows data to be exchanged over a secure channel between two hosts. Encryption provides data confidentiality and data integrity. SSH uses public-key cryptography to authenticate the remote computer and allow the remote host to authenticate the user. This protocol is typically used to login in a remote host and execute commands, but it also supports tunneling, forwarding arbitrary TCP ports and X11 connections. SSH can also be used to transfer files using the associated SFTP or SCP protocols.
Fix	It is recommended to allow connection to this service only from trusted hosts/networks.
Standards	CVE: 1999-0634
Details	SSH-1.99-OpenSSH_3.5p1

■□□□□ SSH Supported Algorithms

Emaze ID	10088
Severity	Info
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	1-gen-2005
Description	The remote host supports the cryptography algorithms listed below.
Fix	It is recommended to configure SSH with Public-key based cryptography algorithms such as: RSA, Diffie-Hellman or DSA.
Details	Compression Algorithms Client To Server: none,zlib Server Host Key Algorithms: ssh-rsa,ssh-dss Encryption Algorithms Client To Server: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour, aes192-cbc,aes256

Confirmed Vulnerabilities Details

-cbc,rijndael-cbc@lysator.liu.se
Kex Algorithms: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
Mac Algorithms Client To Server: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@
openssh.com,hmac-sha1
-96,hmac-md5-96
Cookie: cdeb0aed88cae05ced36be89fa48eb54
Compression Algorithms Server To Server: none,zlib
Mac Algorithms Server To Server: hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@
openssh.com,hmac-sha1
-96,hmac-md5-96
Encryption Algorithms Server To Server: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,
aes192-cbc,aes256
-cbc,rijndael-cbc@lysator.liu.se

■□□□□ SSHv2 Key Fingerprint

Emaze ID	10098
Severity	Info
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	1-gen-2006
Description	This is the remote host SSH Protocol version 2 key fingerprint.
Fix	It is recommended to disable the service if not used.
Details	c6:c5:57:58:81:5c:36:98:02:d4:a6:54:91:df:01:03

■□□□□ SSL Certificate Information

Emaze ID	10070
Severity	Info
Service	🔒 443 / TCP (tcpwrappeds)
Family	MISCELLANEOUS SERVER
Published	1-gen-2005
Description	The Secure Socket Layer protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party Certification Authority (CA) to identify one or both ends of a transaction. It is possible to gather additional remote host information from SSL certificates.
Details	Serial: 0 Issuer: Organization Name: SomeOrganization Email Address: root@localhost.localdomain Locality: SomeCity Country: -- State or Province: SomeState Common Name: localhost.localdomain Organization Unit Name: SomeOrganizationalUnit Pubkey Bits: 1024 Subject Name Hash: 1926435156 Subject: Organization Name: SomeOrganization Email Address: root@localhost.localdomain Locality: SomeCity Country: --

Confirmed Vulnerabilities Details

State or Province: SomeState
Common Name: localhost.localdomain
Organization Unit Name: SomeOrganizationalUnit

SSL Supported Ciphers List

Emaze ID	10069
Severity	Info
Service	443 / TCP (tcpwrappeds)
Family	MISCELLANEOUS SERVER
Published	1-gen-2005
Description	The remote host supports SSL ciphers listed below.
Fix	It is recommended to disable weak ciphers in favor of large encryption keys.
Reference	http://www.openssl.org/docs/apps/ciphers.html
Details	DHE-RSA-AES256-SHA DHE-DSS-AES256-SHA AES256-SHA EDH-RSA-DES-CBC3-SHA EDH-DSS-DES-CBC3-SHA DES-CBC3-SHA DES-CBC3-MD5 DHE-RSA-AES128-SHA DHE-DSS-AES128-SHA AES128-SHA IDEA-CBC-SHA IDEA-CBC-MD5 RC2-CBC-MD5 DHE-DSS-RC4-SHA RC4-SHA RC4-MD5 RC4-MD5 RC4-64-MD5 EXP1024-DHE-DSS-DES-CBC-SHA EXP1024-DES-CBC-SHA EXP1024-RC2-CBC-MD5 EDH-RSA-DES-CBC-SHA EDH-DSS-DES-CBC-SHA DES-CBC-SHA DES-CBC-MD5 EXP1024-DHE-DSS-RC4-SHA EXP1024-RC4-SHA EXP1024-RC4-MD5 EXP-EDH-RSA-DES-CBC-SHA EXP-EDH-DSS-DES-CBC-SHA EXP-DES-CBC-SHA EXP-RC2-CBC-MD5 EXP-RC2-CBC-MD5 EXP-RC4-MD5 EXP-RC4-MD5

SSL Supported Protocols

Emaze ID	10213
Severity	Info

Confirmed Vulnerabilities Details

Service	443 / TCP (tcpwrapped)
Family	MISCELLANEOUS SERVER
Published	1-gen-2007
Description	The Secure Socket Layer protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party Certification Authority (CA) to identify one or both ends of a transaction. The remote host supports SSL protocols listed below.
Details	TLSv1: True SSLv3: True SSLv2: True

Software Installed

Emaze ID	10139
Severity	Info
Family	MISCELLANEOUS SERVER
Published	1-gen-2006
Description	In the following a list of ipLegion software identified on the target host.
Fix	It is recommended to disable not used services.
Details	Detected BIND version 9.2.1 on port 53/udp Detected OpenSSH version 3.5p1 on port 22/tcp Detected vsFTPd version 1.1.3 on port 21/tcp

UNIX RPC Services

Emaze ID	10086
Severity	Info
Service	111 / UDP (rpcbind)
Family	UNIX RPC
Published	1-gen-2005
Description	In the remote host various RPC services are running. These services in the past were affected by multiple vulnerabilities.
Fix	It is recommended to disable these services if not used or allow incoming connections only to untrusted networks.
Standards	CVE: 1999-0632 CVSS: 0.0
Details	Detected mountd version 1 on port 1026/tcp Detected mountd version 1 on port 1027/udp Detected mountd version 2 on port 1026/tcp Detected mountd version 2 on port 1027/udp Detected mountd version 3 on port 1026/tcp Detected mountd version 3 on port 1027/udp Detected nfs version 2 on port 2049/udp Detected nfs version 3 on port 2049/udp Detected nlockmgr version 1 on port 1026/udp Detected nlockmgr version 3 on port 1026/udp Detected nlockmgr version 4 on port 1026/udp Detected rpcbind version 2 on port 111/tcp Detected rpcbind version 2 on port 111/udp Detected rquotad version 1 on port 835/udp Detected rquotad version 1 on port 838/tcp Detected rquotad version 2 on port 835/udp

Confirmed Vulnerabilities Details

Detected rquotad version 2 on port 838/tcp
Detected sgi_fam version 2 on port 1025/tcp
Detected status version 1 on port 1024/tcp
Detected status version 1 on port 1024/udp

■□□□□ UNIX RPC Services

Emaze ID	10086
Severity	Info
Service	111 / TCP (rpcbind)
Family	UNIX RPC
Published	1-gen-2005
Description	In the remote host various RPC services are running. These services in the past were affected by multiple vulnerabilities.
Fix	It is recommended to disable these services if not used or allow incoming connections only to untrusted networks.
Standards	CVE: 1999-0632 CVSS: 0.0
Details	Detected mountd version 1 on port 1026/tcp Detected mountd version 1 on port 1027/udp Detected mountd version 2 on port 1026/tcp Detected mountd version 2 on port 1027/udp Detected mountd version 3 on port 1026/tcp Detected mountd version 3 on port 1027/udp Detected nfs version 2 on port 2049/udp Detected nfs version 3 on port 2049/udp Detected nlockmgr version 1 on port 1026/udp Detected nlockmgr version 3 on port 1026/udp Detected nlockmgr version 4 on port 1026/udp Detected rpcbind version 2 on port 111/tcp Detected rpcbind version 2 on port 111/udp Detected rquotad version 1 on port 835/udp Detected rquotad version 1 on port 838/tcp Detected rquotad version 2 on port 835/udp Detected rquotad version 2 on port 838/tcp Detected sgi_fam version 2 on port 1025/tcp Detected status version 1 on port 1024/tcp Detected status version 1 on port 1024/udp

■□□□□ VMWare Virtual Machine Running

Emaze ID	10156
Severity	Info
Family	CLIENT SIDE
Published	1-gen-2006
Description	The remote host is a VMWare virtual machine.
Fix	It is recommended to disable the service if not used.

Potential Vulnerabilities by Severity

Severity	Vulnerability	Port	Status
High	OpenSSL Public Key Processing Denial of Service Vulnerability	53/UDP	New
High	OpenSSL ASN.1 Structures Denial of Service Vulnerability	53/UDP	New
High	OpenSSH Buffer Mismanagement Vulnerabilities	22/TCP	New
High	Multiple Vendor libc DNS Resolver Buffer Overflow Vulnerability	53/UDP	New
High	ISC BIND Multiple Remote Denial of Service Vulnerabilities	53/UDP	New
High	ISC BIND 9 Remote Cache Poisoning Vulnerability	53/UDP	New
Medium	OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability	22/TCP	New
Medium	OpenSSH GSSAPI Credential Disclosure Vulnerability	22/TCP	New
Medium	Multiple Vendors BIND 'inet_network()' Off-by-One Buffer Overflow Vulnerability	53/UDP	New
Medium	Multiple DNS Server 'NXDomain' Denial Of Service Vulnerability	53/UDP	New
Medium	ISC BIND TSIG Zone Transfer Denial Of Service Vulnerability	53/UDP	New
Medium	ISC BIND Remote Fetch Context Denial of Service Vulnerability	53/UDP	New
Medium	ISC BIND Remote DNSSEC Validation Denial of Service Vulnerability	53/UDP	New
Low	OpenSSL PKCS Padding RSA Signature Forgery Vulnerability	53/UDP	New
Low	OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability	22/TCP	New
Low	OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability	22/TCP	New
Low	OpenSSH X connections Session Hijacking Vulnerability	22/TCP	New
Low	OpenSSH Remote Root Authentication Timing Side-Channel Vulnerability	22/TCP	New
Low	OpenSSH PAM Conversation Memory Scrubbing Vulnerability	22/TCP	New

*The status field is a synthesis of any change that may have occurred between the current and the previous activity. Possible values are: **New**, if the vulnerability wasn't found in the previous activity and was found in the current one. **Already known**, if the vulnerability was found both in the previous and in the current activity. **Removed**, if the vulnerability found in the previous activity wasn't found in the current one. **Port closed**, if the appliance, for some reason, couldn't check in the current activity for a vulnerability that was found in the previous one.*

Potential Vulnerabilities by Port

Protocol	Port	Service	Vulnerability
TCP			
	22	ssh	OpenSSH Buffer Mismanagement Vulnerabilities
	22	ssh	OpenSSH GSSAPI Credential Disclosure Vulnerability
	22	ssh	OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability
	22	ssh	OpenSSH PAM Conversation Memory Scrubbing Vulnerability
	22	ssh	OpenSSH Remote Root Authentication Timing Side-Channel Vulnerability
	22	ssh	OpenSSH X connections Session Hijacking Vulnerability
	22	ssh	OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability
	22	ssh	OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability
UDP			
	53	domain	ISC BIND 9 Remote Cache Poisoning Vulnerabilit
	53	domain	ISC BIND Multiple Remote Denial of Service Vulnerabilities
	53	domain	ISC BIND Remote DNSSEC Validation Denial of Service Vulnerability
	53	domain	ISC BIND Remote Fetch Context Denial of Servic Vulnerability
	53	domain	ISC BIND TSIG Zone Transfer Denial Of Service Vulnerability
	53	domain	Multiple DNS Server 'NXDomain' Denial Of Service Vulnerability
	53	domain	Multiple Vendor libc DNS Resolver Buffer Overflow Vulnerability
	53	domain	Multiple Vendors BIND 'inet_network()' Off-by-One Buffer Overflow Vulnerability
	53	domain	OpenSSL ASN.1 Structures Denial of Service Vulnerability
	53	domain	OpenSSL PKCS Padding RSA Signature Forgery Vulnerability
	53	domain	OpenSSL Public Key Processing Denial of Service Vulnerability

Potential Vulnerabilities Details

◣◣◣◣□ **OpenSSH Buffer Mismanagement Vulnerabilities**

Emaze ID	11255
Severity	Potentially High
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	16-set-2003
Description	The 'buffer.c' source file in OpenSSH is exposed to a mismanagement vulnerability. A successf exploitation of this issue might allow an attacker to execute arbitrary code with the privilege of OpenSSH service or cause a Denial of Service conditions.
Fix	It is recommended to update to the latest fixed version available from vendor website: http://www.openssh.com
Reference	http://www.cisco.com/warp/public/707/cisco-sa-20030917-openssh.shtml
Details	Detected OpenSSH version 3.5p1 on port 22/tcp

◣◣◣◣□ **Multiple Vendor libc DNS Resolver Buffer Overflow Vulnerability**

Emaze ID	11584
Severity	Potentially High
Service	53 / UDP (domain)
Family	WEB APPLICATION
Published	26-giu-2002
Description	Due to a flaw in handling maliciuos DNS responces, some implementation of DNS query routin in 'libc' library are affected by a buffer overflow vulnerabilit An attacker may reply in a malicius manner to a DNS lookup request in order to trigger thi issue abd so to deny services to legitimate users or to execute arbitrary code.
Fix	Upgrade to the lasted fixed version available at the vendor website.
Details	Detected BIND version 9.2.1 on port 53/udp

◣◣◣◣□ **ISC BIND Multiple Remote Denial of Service Vulnerabilities**

Emaze ID	14083
Severity	Potentially High
Service	53 / UDP (domain)
Family	DNS SERVERS
Published	5-set-2006
Description	ISC BIND is affected by multiple Denial of Service vulnerabilities. A successful exploitation c these issues might allow an attacker to cause Denial of Service conditions, effectively denyin service to legitimate users.
Fix	Download the latest stable release from vendor website: http://www.isc.org/
Reference	http://www.isc.org/index.pl?/sw/bind/bind-security.php http://www.isc.org/products/BIND/ http://www.isc.org/index.pl?/sw/bind/bind9.3.php http://www.kb.cert.org/vuls/id/697164 http://www.kb.cert.org/vuls/id/915404
Details	Detected BIND version 9.2.1 on port 53/udp

Potential Vulnerabilities Details

OpenSSL ASN.1 Structures Denial of Service Vulnerability

Emaze ID	14153
Severity	Potentially High
Service	53 / UDP (domain)
Family	MISCELLANEOUS SERVER
Published	28-set-2006
Description	OpenSSL is affected by a Denial of Service vulnerability. A successful exploitation of this issu might allow an attacker to cause applications that use the vulnerable library to consum excessive CPU and memory resources and crash, denying further access to users.
Fix	Download the latest stable release from vendor website: http://www.openssl.org/
Reference	http://www.kb.cert.org/vuls/id/247744 http://www.openssl.org/news/secadv_20060928.txt
Details	Detected BIND version 9.2.1 on port 53/udp

OpenSSL Public Key Processing Denial of Service Vulnerability

Emaze ID	14154
Severity	Potentially High
Service	53 / UDP (domain)
Family	MISCELLANEOUS SERVER
Published	28-set-2006
Description	Due to a lack of validation of the lengths of public keys being used, OpenSSL is affected by Denial of Service vulnerability. A successful exploitation of this issue might allow an attacker t crash an affected server using OpenSSL.
Fix	Download the latest stable release from vendor website: http://www.openssl.org/
Reference	http://www.openssl.org/news/secadv_20060928.txt
Details	Detected BIND version 9.2.1 on port 53/udp

ISC BIND 9 Remote Cache Poisoning Vulnerability

Emaze ID	15233
Severity	Potentially High
Service	53 / UDP (domain)
Family	DNS SERVERS
Published	24-lug-2007
Description	ISC BIND 9 is affected by a cache poisoning vulnerability. A successful exploitation of this issu might allow an attacker to manipulate cache data, potentially facilitating man-in-the-middle site-impersonation, or Denial of Service attacks.
Fix	Download the latest stable release from vendor website: http://www.isc.org/products/BIND/
Exploit	http://www.securityfocus.com/data/vulnerabilities/exploits/25037-reconstruction.pl http://www.securityfocus.com/data/vulnerabilities/exploits/25037-prediction.pl http://www.securityfocus.com/data/vulnerabilities/exploits/25037.py

Potential Vulnerabilities Details

Reference	http://www.trusteer.com/docs/bind9dns.html http://sunsolve.sun.com/search/document.do?assetkey=1-26-103018-1&searchclause= http://www.kb.cert.org/vuls/id/252735 http://www.securityfocus.com/archive/1/474516
Details	Detected BIND version 9.2.1 on port 53/udp

◣◣◣□□ Multiple DNS Server 'NXDomain' Denial Of Service Vulnerability

Emaze ID	11586
Severity	Potentially Medium
Service	53 / UDP (domain)
Family	DNS SERVERS
Published	27-mar-2003
Description	Due to a flaw in handling malicious DNS requests, some DNS server are affected by a Denial c Service vulnerability. A successful exploitation of this issue allows an attacker to deny service t legitimate users.
Fix	Upgrade to the lasted fixed version available at the vendor website.
Standards	BID: 7217
Details	Detected BIND version 9.2.1 on port 53/udp

◣◣◣□□ OpenSSH GSSAPI Credential Disclosure Vulnerability

Emaze ID	12511
Severity	Potentially Medium
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	31-ago-2005
Description	OpenSSH is susceptible to a GSSAPI credential delegation vulnerability. A remote attacker ma gain access to GSSAPI credentials and utilize them to access resources granted to the origina administrator. This vulnerability is exploitable only if a user has GSSAPI authenticatio configured and 'GSSAPIDelegateCredentials' enabled.
Fix	Download the latest fixed version available from vendor website: http://www.openssh.com/
Reference	http://www.mindrot.org/pipermail/openssh-unix-announce/2005-September/000083.html
Details	Detected OpenSSH version 3.5p1 on port 22/tcp

◣◣◣□□ OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability

Emaze ID	12695
Severity	Potentially Medium
Service	22 / TCP (ssh)
Family	MISCELLANEOUS SERVER
Published	27-gen-2004
Description	An attacker, when LoginGraceTime, MaxStartups and UsePrivilegeSeparation are enabled coul explit a vulnerability that cuses the server to refuse further remote connection attempts, s legitimate users could not use the SSH service.
Fix	Download the latest fixed version available from vendor website: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/
Reference	http://marc.theaimsgroup.com/?l=openssh-unix-dev&m=107520317020444&w=2 http://marc.theaimsgroup.com/?l=openssh-unix-dev&m=107529205602320&w=2 http://rhn.redhat.com/errata/RHSA-2005-550.html

Potential Vulnerabilities Details

Details	Detected OpenSSH version 3.5p1 on port 22/tcp

ISC BIND TSIG Zone Transfer Denial Of Service Vulnerability

Emaze ID	13523
Severity	Potentially Medium
Service	53 / UDP (domain)
Family	DNS SERVERS
Published	24-apr-2006
Description	Due to an application failure to properly handle malformed Secret Key Transactio Authentication (TSIG) replies, ISC BIND is affected by a remote Denial of Service vulnerability An attacker can exploit this issue sending messages with a correct TSIG during a zone transfe to crash the affected service denying service to legitimate users.
Fix	Download the latest stable version at vendor website: http://www.isc.org
Exploit	You can use PROTOS DSN Test Suite developed by Oulu Unversity Secure Programming Group to exploit this issue.
Reference	http://www.isc.org/index.pl?/sw/bind/bind-security.php
Details	Detected BIND version 9.2.1 on port 53/udp

ISC BIND Remote DNSSEC Validation Denial of Service Vulnerability

Emaze ID	14576
Severity	Potentially Medium
Service	53 / UDP (domain)
Family	DNS SERVERS
Published	25-gen-2007
Description	ISC BIND is affected by a remote Denial of Service vulnerability. A successful exploitation of th issue might allow an attacker to crash the affected application, denying any further access.
Fix	Download the latest stable release from vendor website: http://www.isc.org/products/BIND/
Reference	http://marc.theaimsgroup.com/?l=bind-announce&m=116968687928814&w=2 http://marc.theaimsgroup.com/?l=bind-announce&m=116968686102367&w=2 http://marc.theaimsgroup.com/?l=bind-announce&m=116968787232345&w=2 http://www.isc.org/index.pl?/sw/bind/bind-security.php http://marc.theaimsgroup.com/?l=bind-announce&m=116968519300764&w=2
Details	Detected BIND version 9.2.1 on port 53/udp

ISC BIND Remote Fetch Context Denial of Service Vulnerability

Emaze ID	14577
Severity	Potentially Medium
Service	53 / UDP (domain)
Family	DNS SERVERS
Published	25-gen-2007
Description	ISC BIND is affected by a remote Denial of Service vulnerability. A successful exploitation of th issue might allow an attacker to crash the affected application, denying any further access.
Fix	Download the latest stable release from vendor website: http://www.isc.org/products/BIND/

Potential Vulnerabilities Details

Reference http://marc.theaimsgroup.com/?l=bind-announce&m=116968687928814&w=2
http://marc.theaimsgroup.com/?l=bind-announce&m=116968686102367&w=2
http://marc.theaimsgroup.com/?l=bind-announce&m=116968787232345&w=2
http://www.isc.org/index.pl?/sw/bind/bind-security.php
http://marc.theaimsgroup.com/?l=bind-announce&m=116968519321296&w=2

Details Detected BIND version 9.2.1 on port 53/udp

Multiple Vendors BIND 'inet_network()' Off-by-One Buffer Overflow Vulnerability

Emaze ID 15544

Severity Potentially Medium

Service 53 / UDP (domain)

Family DNS SERVERS

Published 14-gen-2008

Description The application BIND does not properly perform boundary checks on user supplied input data As a consequence input data are copied to an insufficiently sized memory buffer. Th vulnerability has been reported in the 'inet_network()' function. A successful exploitation of thi issue might allow an attacker to execute arbitrary code in the context of the affecte application or cause denial of service conditions.

Fix It is recommended to download the latest stable release from vendor website:
http://www.isc.org/index.pl?/sw/bind/index.php

Reference http://www.kb.cert.org/vuls/id/203611
http://www.kb.cert.org/vuls/id/927905
http://www.isc.org/index.pl?/sw/bind/bind-security.php

Details Detected BIND version 9.2.1 on port 53/udp

OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability

Emaze ID 11139

Severity Potentially Low

Service 22 / TCP (ssh)

Family REMOTE ADMINISTRATION

Published 30-nov-2004

Description Portable version of OpenSSH is affected by an information disclosure vulnerability. An attacke may exploit this issue in order to obtain valid usernames for later time attacks.

Fix Update to the latest fixed version available from vendor website:
http://www.openssh.com

Exploit http://www.securityfocus.com/data/vulnerabilities/exploits/OpenSSH_sshtime_rexp.sh

Details Detected OpenSSH version 3.5p1 on port 22/tcp

OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability

Emaze ID 11253

Severity Potentially Low

Service 22 / TCP (ssh)

Family REMOTE ADMINISTRATION

Published 30-apr-2003

Description OpenSSH-portable consumes different time to authenticate a valid or invalid username, thi issue allows a remote user to identify whether a supplied username is valid.

Potential Vulnerabilities Details

Fix	Update to the latest fixed version available from vendor website: http://www.openssh.com
Exploit	Two examples of exploit are avaiable at: http://www.securityfocus.com/data/vulnerabilities/exploits/ssh_brute.c http://www.securityfocus.com/data/vulnerabilities/exploits/gossh.sh
Reference	http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=281595
Details	Detected OpenSSH version 3.5p1 on port 22/tcp

OpenSSH Remote Root Authentication Timing Side-Channel Vulnerability

Emaze ID	11254
Severity	Potentially Low
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	1-mag-2003
Description	OpenSSH-portable is vulnerable to a timing attack that may allow a remote user to obtain th administrative password and so to gain unauthorized access to OpenSSH server.
Fix	Update to the latest fixed version available from vendor website: http://www.openssh.com
Reference	http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=281595
Details	Detected OpenSSH version 3.5p1 on port 22/tcp

OpenSSH PAM Conversation Memory Scrubbing Vulnerability

Emaze ID	11257
Severity	Potentially Low
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	12-nov-2003
Description	A design error causes OpenSSH to fail to handle aborted conversations with PAM modules. Th memory may not be cleaned by sensitive information making OpenSSH vulnerable t information disclosure.
Fix	Update to the latest fixed version available from vendor website: http://www.openssh.com
Exploit	Currently we are not aware of any exploits for this issue. If you feel we are in error or are awar of more recent information, please mail us at: vuln_rep@emaze.net
Reference	http://www.securityfocus.com/archive/1/344435
Standards	BID: 9040
Details	Detected OpenSSH version 3.5p1 on port 22/tcp

OpenSSL PKCS Padding RSA Signature Forgery Vulnerability

Emaze ID	14082
Severity	Potentially Low
Service	53 / UDP (domain)
Family	MISCELLANEOUS SERVER
Published	5-set-2006

Potential Vulnerabilities Details

Description	OpenSSL is affected by a vulnerability that may allow an RSA signature to be forged. malicious user might forge a PKCS #1 v1.5 signature when an RSA key with exponent 3 is use leading to sign digital certificates or RSA keys and takes advantage of trust relationships whic depend on these credentials.
Fix	Download the latest stable release from vendor website: http://www.openssl.org/
Reference	http://www.imc.org/ietf-openpgp/mail-archive/msg14307.html
Details	Detected BIND version 9.2.1 on port 53/udp

OpenSSH X connections Session Hijacking Vulnerability

Emaze ID	15703
Severity	Potentially Low
Service	22 / TCP (ssh)
Family	REMOTE ADMINISTRATION
Published	25-mar-2008
Description	The application OpenSSH is prone to a vulnerability that allows attackers to hijack forwarded connections. A successful exploitation of this issue might allow an attacker to run arbitrary she commands with the privileges of the user running the affected application.
Fix	It is recommended to download the latest stable release from vendor website: http://www.openssh.com/
Reference	http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
Details	Detected OpenSSH version 3.5p1 on port 22/tcp

Legend

Label Description

Exposure Level:	a synthetic benchmark describing the security state of a host. Possible values are: LOW, MEDIUM, HIGH, CRITICAL.
Exposed Host:	a host is exposed when its exposure level is HIGH or CRITICAL.
Confirmed Vulnerabilities:	is detected analysing the host response to such ad hoc request. By consequence, the installed software has a security flaw that may be exploited by an attacker
Potential Vulnerabilities:	is detected analysing the software version contained in the banner of the application response.

Severity Level Description

Vulnerabilities are classified by severity level. There are currently five severity levels: critical, high, medium, low, info.

Critical	A Critical Severity Vulnerability is similar to an High Severity Vulnerability, but it's an especially easy one to exploit. It allows any user with a minimum of technical skill to compromise the affected system. Two kinds of vulnerabilities fall into this category: those that are trivial to exploit (e.g. blank or easy passwords), or those which have an exploit available out of the box in a penetration testing tool (e.g. Metasploit, Core Impact).
High	A High Severity Vulnerability permits a malicious user to directly interfere, at the administrative (root) level, with the structure and functions of the target system via a single vulnerability. Examples of High Severity Vulnerabilies are those which permit a malicious user to access a target system and allows him/her to steal, alter or delete sensitive data stored on it, or to run arbitrary programs.
Medium	A Medium Severity Vulnerability permits a malicious user to externally tamper with the normal operations of a target. Examples of Medium Severity Vulnerabilities are those which let a malicious user mount a Denial of Service (DoS) attack against a target system or access its data.
Low	A Low Severity Vulnerability may help a malicious user to organize an exploit on a target system. However, by itself, it does not constitute a direct breach of the system's security.
Info	These are not technical problems as they are legitimate operations. However, a malicious user can take advantage of these situations to gain useful information which can then be used to form an attack strategy. When deciding whether the service should be kept open or closed, the System Manager will have to judge every case individually.