



**tenable**<sup>®</sup> Nessus

# Meta

Report generated by Tenable Nessus<sup>™</sup>

Wed, 04 Dec 2024 09:38:32 EST

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.50.100.....	4
• 192.168.50.101.....	8

Nessus Essentials

---

## Vulnerabilities by Host

---

192.168.50.100



## Vulnerabilities

Total: 68

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	9.8	-	-	201969	Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 2024 Security Releases).
MEDIUM	8.2	-	-	192945	Node.js 18.x < 18.20.1 / 20.x < 20.12.1 / 21.x < 21.7.2 Multiple Vulnerabilities (Wednesday, April 3, 2024 Security Releases).
MEDIUM	7.9	-	-	190856	Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Release).
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	4.8	-	-	197900	Intel Media SDK Multiple Vulnerabilities (INTEL-SA-00935)
INFO	N/A	-	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	182774	Curl Installed (Linux / Unix)
INFO	N/A	-	-	55472	Device Hostname
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	159273	Dockerfile Detection for Linux/UNIX
INFO	N/A	-	-	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	-	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	-	33276	Enumerate MAC Addresses via SSH
INFO	N/A	-	-	170170	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	-	179200	Enumerate the Network Routing configuration via SSH

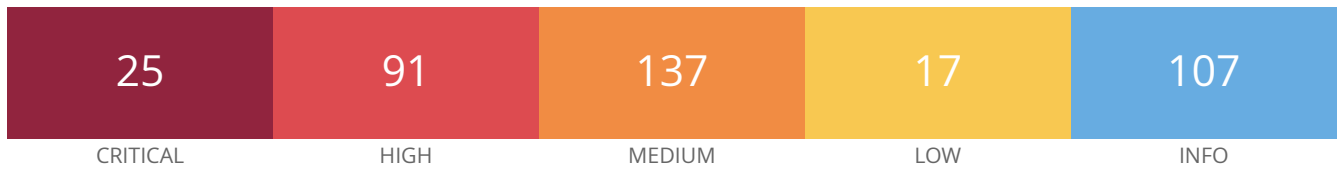
INFO	N/A	-	-	<a href="#">168980</a>	Enumerate the PATH Variables
INFO	N/A	-	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	-	<a href="#">204827</a>	Exiv2 Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">168982</a>	Filepaths contain Dangerous characters (Linux)
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	<a href="#">171410</a>	IP Assignment Method Detection
INFO	N/A	-	-	<a href="#">197894</a>	Intel Media SDK Installed (Linux)
INFO	N/A	-	-	<a href="#">147817</a>	Java Detection and Identification (Linux / Unix)
INFO	N/A	-	-	<a href="#">189990</a>	Jmcnamara Spreadsheet-ParseExcel Installed (Unix)
INFO	N/A	-	-	<a href="#">151883</a>	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	-	-	<a href="#">200214</a>	Libndp Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">157358</a>	Linux Mounted Devices
INFO	N/A	-	-	<a href="#">193143</a>	Linux Time Zone Information
INFO	N/A	-	-	<a href="#">95928</a>	Linux User List Enumeration
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">10147</a>	Nessus Server Detection
INFO	N/A	-	-	<a href="#">64582</a>	Netstat Connection Information
INFO	N/A	-	-	<a href="#">14272</a>	Netstat Portscanner (SSH)
INFO	N/A	-	-	<a href="#">178771</a>	Node.js Installed (Linux / UNIX)
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">97993</a>	OS Identification and Installed Software Enumeration over SSH (Using New SSH Library)
INFO	N/A	-	-	<a href="#">117887</a>	OS Security Patch Assessment Available
INFO	N/A	-	-	<a href="#">148373</a>	OpenJDK Java Detection (Linux / Unix)

INFO	N/A	-	-	<a href="#">168007</a>	OpenSSL Installed (Linux)
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	-	<a href="#">130024</a>	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	-	<a href="#">45405</a>	Reachable IPv6 address
INFO	N/A	-	-	<a href="#">202184</a>	Ruby Programming Language Installed (Linux)
INFO	N/A	-	-	<a href="#">174788</a>	SQLite Local Detection (Linux)
INFO	N/A	-	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	-	<a href="#">22869</a>	Software Enumeration (SSH)
INFO	N/A	-	-	<a href="#">42822</a>	Strict Transport Security (STS) Detection
INFO	N/A	-	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	<a href="#">138330</a>	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	<a href="#">110095</a>	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	-	<a href="#">141118</a>	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	-	<a href="#">163326</a>	Tenable Nessus Installed (Linux)
INFO	N/A	-	-	<a href="#">56468</a>	Time of Last System Startup
INFO	N/A	-	-	<a href="#">192709</a>	Tukaani XZ Utils Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">110483</a>	Unix / Linux Running Processes Information
INFO	N/A	-	-	<a href="#">152742</a>	Unix Software Discovery Commands Available
INFO	N/A	-	-	<a href="#">189731</a>	Vim Installed (Linux)
INFO	N/A	-	-	<a href="#">182848</a>	libcurl Installed (Linux / Unix)

INFO	N/A	-	-	204828	libexiv2 Installed (Linux / Unix)
INFO	N/A	-	-	136340	nginx Installed (Linux/UNIX)

\* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.50.101



## Vulnerabilities

Total: 377

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	77823	Bash Remote Code Execution (Shellshock)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	-	-	32320	Weak Debian OpenSSH Keys in ~/.ssh/authorized_keys
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	-	-	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	-	-	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	32432	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities (USN-613-1)
CRITICAL	10.0*	-	-	37936	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilities (USN-644-1)
CRITICAL	10.0*	-	-	33531	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-625-1)
CRITICAL	10.0*	-	-	36916	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libxml2 vulnerabilities (USN-673-1)
CRITICAL	10.0*	-	-	36454	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux-source-2.6.15/22, linu vulnerabilities (USN-714-1)
CRITICAL	10.0*	-	-	44399	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-894-1)
CRITICAL	10.0*	-	-	39800	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dhcp3 vulnerability (USN-803-1)



CRITICAL	10.0*	-	-	<a href="#">40576</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libxml2 vulnerabilities (USN-815-1)
CRITICAL	10.0*	-	-	<a href="#">37762</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : apt vulnerabilities (USN-762-1)
CRITICAL	10.0*	-	-	<a href="#">50044</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : linux, linux-ec2, linux-source-2.6.15 vulnerabilities (USN-1000-1)
CRITICAL	10.0*	-	-	<a href="#">49805</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : openssl vulnerabilities (USN-1003-1)
CRITICAL	10.0*	-	-	<a href="#">37337</a>	Ubuntu 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.22 vulnerabilities (USN-751-1)
CRITICAL	10.0*	-	-	<a href="#">58444</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : freetype vulnerabilities (USN-1403-1)
CRITICAL	10.0*	-	-	<a href="#">58743</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : samba vulnerabilities (USN-1423-1)
CRITICAL	10.0*	-	-	<a href="#">40529</a>	Ubuntu 8.04 LTS / 8.10 / 9.04 : apr vulnerability (USN-813-1)
CRITICAL	10.0*	-	-	<a href="#">40531</a>	Ubuntu 8.04 LTS / 8.10 / 9.04 : apr-util vulnerability (USN-813-3)
CRITICAL	10.0*	-	-	<a href="#">56388</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1225-1)
CRITICAL	10.0*	-	-	<a href="#">61708</a>	VNC Server 'password' Password
HIGH	9.8	-	-	<a href="#">134862</a>	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	6.8	-	-	<a href="#">56583</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1236-1)
HIGH	7.2*	-	-	<a href="#">34048</a>	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-637-1)
HIGH	7.5*	-	-	<a href="#">33504</a>	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : pcre3 vulnerability (USN-624-1)
HIGH	9.3*	-	-	<a href="#">33388</a>	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : samba regression (USN-617-2)
HIGH	9.3*	-	-	<a href="#">33217</a>	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : samba vulnerabilities (USN-617-1)
HIGH	7.8*	-	-	<a href="#">37683</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.15/22 vulnerabilities (USN-679-1)
HIGH	7.2*	-	-	<a href="#">37654</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : shadow vulnerability (USN-695-1)

HIGH	7.2*	-	-	<a href="#">36530</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : udev vulnerabilities (USN-758-1)
HIGH	7.2*	-	-	<a href="#">37886</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : vm-builder vulnerabi (USN-670-1)
HIGH	9.3*	-	-	<a href="#">36681</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/2.6.15.2 vulnerabilities (USN-659-1)
HIGH	7.5*	-	-	<a href="#">42858</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : apache2 vulnerabilities (USN-860-1)
HIGH	7.8*	-	-	<a href="#">43026</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-864-1)
HIGH	8.5*	-	-	<a href="#">44585</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : mysql-dfsg-5.0.9, mysql-dfsg-5.1 vulnerabilities (USN-897-1)
HIGH	7.1*	-	-	<a href="#">40655</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 regression (USN-802-2)
HIGH	7.8*	-	-	<a href="#">39371</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 vulnerability (USN-787-1)
HIGH	7.1*	-	-	<a href="#">39789</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 vulnerability (USN-802-1)
HIGH	7.2*	-	-	<a href="#">38984</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : cron vulnerability (USN-778-1)
HIGH	7.5*	-	-	<a href="#">40657</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : curl vulnerability (USN-818-1)
HIGH	7.5*	-	-	<a href="#">39515</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : cyrus-sasl2 vulnerability (USN-790-1)
HIGH	7.5*	-	-	<a href="#">40656</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : gnutls12, gnutls13, gnutls26 vulnerabilities (USN-809-1)
HIGH	7.8*	-	-	<a href="#">39586</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-793-1)
HIGH	7.8*	-	-	<a href="#">40416</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-807-1)
HIGH	7.8*	-	-	<a href="#">42209</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-852-1)

HIGH	7.2*	-	-	<a href="#">40658</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-819-1)
HIGH	9.3*	-	-	<a href="#">41968</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : samba vulnerabilities (USN-839-1)
HIGH	9.3*	-	-	<a href="#">48361</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : freetype vulnerabilities (USN-972-1)
HIGH	7.5*	-	-	<a href="#">46731</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : glibc, eglibc vulnerabilities (USN-944-1)
HIGH	7.5*	-	-	<a href="#">47695</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libpng vulnerabilities (USN-960-1)
HIGH	7.8*	-	-	<a href="#">46810</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15 vulnerabilities (USN-947-1)
HIGH	7.2*	-	-	<a href="#">49283</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15 vulnerabilities (USN-988-1)
HIGH	7.2*	-	-	<a href="#">48381</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15, {ec2,fsl-imx51,mvl-dove,source-2.6.15,ti-omap} vulnerabilities (USN-974-1)
HIGH	7.2*	-	-	<a href="#">48253</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15, {source-2.6.15,ec2,mvl-dove,ti-omap} vulnerabilities (USN-966-1)
HIGH	7.5*	-	-	<a href="#">49306</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : php5 vulnerabilities (USN-989-1)
HIGH	8.5*	-	-	<a href="#">46700</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : postgresql-8.3, postgresql-8.4 vulnerabilities (USN-942-1)
HIGH	7.5*	-	-	<a href="#">49236</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : samba vulnerability (USN-987-1)
HIGH	7.5*	-	-	<a href="#">47035</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 : samba vulnerability (USN-987-1)
HIGH	7.5*	-	-	<a href="#">55087</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 / 11.04 : perl regressions (USN-1126-2)
HIGH	7.5*	-	-	<a href="#">55086</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 / 11.04 : perl vulnerabilities (USN-1126-1)
HIGH	7.9*	-	-	<a href="#">50490</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : cups, cups-filters vulnerability (USN-1012-1)

HIGH	7.5*	-	-	<a href="#">53372</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : dhcp3 vulnerability (USN-1108-1)
HIGH	9.3*	-	-	<a href="#">50491</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : freetype vulnerabilities (USN-1013-1)
HIGH	9.3*	-	-	<a href="#">52667</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff regression (USN-1085-2)
HIGH	9.3*	-	-	<a href="#">52581</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff vulnerabilities (USN-1085-1)
HIGH	7.8*	-	-	<a href="#">32359</a>	Ubuntu 7.04 / 7.10 / 8.04 LTS : openssh update (USN-612-5)
HIGH	7.8*	-	-	<a href="#">65109</a>	Ubuntu 7.04 / 7.10 / 8.04 LTS : openssh vulnerability (USN-612-4)
HIGH	7.8*	-	-	<a href="#">32358</a>	Ubuntu 7.04 / 7.10 / 8.04 LTS : ssl-cert vulnerability (USN-612-3)
HIGH	8.3*	-	-	<a href="#">37161</a>	Ubuntu 7.10 / 8.04 LTS : linux-ubuntu-modules-2.6.22/24 vulnerability (USN-662-2)
HIGH	7.5*	-	-	<a href="#">58318</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : eglibc, glibc vulnerabilities (USN-1396-1)
HIGH	9.3*	-	-	<a href="#">56870</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : freetype vulnerabilities (USN-1267-1)
HIGH	7.5*	-	-	<a href="#">57998</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerabilities (USN-1367-1)
HIGH	9.3*	-	-	<a href="#">57615</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libxml2 vulnerabilities (USN-1334-1)
HIGH	8.5*	-	-	<a href="#">58325</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1397-1)
HIGH	9.3*	-	-	<a href="#">57887</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : openssl vulnerabilities (USN-1357-1)
HIGH	7.5*	-	-	<a href="#">57932</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 regression (USN-1358-2)
HIGH	7.5*	-	-	<a href="#">56554</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerabilities (USN-1231-1)
HIGH	7.5*	-	-	<a href="#">57888</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerabilities (USN-1358-1)

HIGH	7.8*	-	-	<a href="#">56048</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apache2 vulnerabilities (USN-1199-1)
HIGH	N/A	-	-	<a href="#">56281</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apt vulnerabilities (USN-1215-1)
HIGH	7.5*	-	-	<a href="#">55414</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : curl vulnerabilities (USN-1158-1)
HIGH	9.3*	-	-	<a href="#">55168</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : libxml2 vulnerabilities (USN-1153-1)
HIGH	N/A	-	-	<a href="#">59526</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : apt updates (USN-1475-1)
HIGH	7.8*	-	-	<a href="#">62495</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : bind9 vulnerability (USN-1601-1)
HIGH	N/A	-	-	<a href="#">62179</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : gnupg gnupg2 vulnerability (USN-1570-1)
HIGH	7.5*	-	-	<a href="#">59016</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : php5 vulnerability (USN-1437-1)
HIGH	7.2*	-	-	<a href="#">59170</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : sudo vulnerability (USN-1442-1)
HIGH	7.5*	-	-	<a href="#">59856</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : tiff vulnerabilities (USN-1498-1)
HIGH	7.5*	-	-	<a href="#">63109</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : perl vulnerabilities (USN-1643-1)
HIGH	7.5*	-	-	<a href="#">65629</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : perl vulnerability (USN-1770-1)
HIGH	8.5*	-	-	<a href="#">65818</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1789-1)
HIGH	7.8*	-	-	<a href="#">39363</a>	Ubuntu 8.04 LTS / 8.10 / 9.04 : apr-util vulnerabilities (USN-786-1)
HIGH	7.2*	-	-	<a href="#">50318</a>	Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : glibc, eglibc vulnerabilities (USN-1009-1)
HIGH	7.2*	-	-	<a href="#">51501</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : eglibc, glibc vulnerability (USN-1009-2)

HIGH	7.6*	-	-	<a href="#">50649</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openssl vulnerability (USN-1018-1)
HIGH	7.6*	-	-	<a href="#">52529</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : pango1.0 vulnerability (USN-1082-1)
HIGH	7.2*	-	-	<a href="#">48904</a>	Ubuntu 8.04 LTS : linux regression (USN-974-2)
HIGH	7.9*	-	-	<a href="#">52475</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1072-1)
HIGH	7.8*	-	-	<a href="#">53303</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1105-1)
HIGH	7.1*	-	-	<a href="#">55094</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1133-1)
HIGH	7.2*	-	-	<a href="#">55109</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1146-1)
HIGH	7.1*	-	-	<a href="#">55607</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1170-1)
HIGH	7.8*	-	-	<a href="#">55922</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1189-1)
HIGH	7.2*	-	-	<a href="#">56911</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1268-1)
HIGH	7.2*	-	-	<a href="#">57055</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1291-1)
HIGH	7.2*	-	-	<a href="#">58271</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1390-1)
HIGH	7.2*	-	-	<a href="#">59816</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1493-1)
HIGH	7.8*	-	-	<a href="#">59985</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1507-1)
HIGH	7.8*	-	-	<a href="#">33093</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-614-1)
HIGH	7.2*	-	-	<a href="#">62474</a>	Ubuntu 8.04 LTS : linux vulnerability (USN-1598-1)
HIGH	7.9*	-	-	<a href="#">58131</a>	Ubuntu 8.04 LTS : samba vulnerability (USN-1374-1)
HIGH	7.5*	-	-	<a href="#">10205</a>	rlogin Service Detection
MEDIUM	8.6	-	-	<a href="#">136769</a>	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	7.5	-	-	<a href="#">42256</a>	NFS Shares World Readable
MEDIUM	7.5	-	-	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	7.5	-	-	<a href="#">90509</a>	Samba Badlock Vulnerability
MEDIUM	6.5	-	-	<a href="#">139915</a>	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted

MEDIUM	6.5	-	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	<a href="#">42263</a>	Unencrypted Telnet Server
MEDIUM	5.9	-	-	<a href="#">136808</a>	ISC BIND Denial of Service
MEDIUM	5.9	-	-	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	-	-	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	-	-	<a href="#">12217</a>	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	-	-	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	3.4	-	-	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0*	-	-	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	-	-	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREEBIE)
MEDIUM	4.6*	-	-	<a href="#">36805</a>	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : dbus vulnerabilities (USN-653-1)
MEDIUM	4.3*	-	-	<a href="#">34094</a>	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerability (USN-640-1)
MEDIUM	6.2*	-	-	<a href="#">33941</a>	Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : postfix vulnerability (USN-636-1)
MEDIUM	6.8*	-	-	<a href="#">37148</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : curl vulnerability (USN-726-1)

MEDIUM	4.3*	-	-	<a href="#">37045</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : gnutls12, gnutls13, gnutls26 regression (USN-678-2)
MEDIUM	4.3*	-	-	<a href="#">37965</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : gnutls12, gnutls13, gnutls26 vulnerability (USN-678-1)
MEDIUM	5.8*	-	-	<a href="#">36382</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : openssl vulnerability (USN-704-1)
MEDIUM	5.0*	-	-	<a href="#">36907</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : openssl vulnerability (USN-750-1)
MEDIUM	5.0*	-	-	<a href="#">36589</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : apache2 vulnerabilities (USN-731-1)
MEDIUM	4.6*	-	-	<a href="#">37299</a>	Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : mysql-dfsg-5.0 vulnerability (USN-671-1)
MEDIUM	4.3*	-	-	<a href="#">55095</a>	Ubuntu 6.06 LTS / 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apache apr vulnerabilities (USN-1134-1)
MEDIUM	6.8*	-	-	<a href="#">55092</a>	Ubuntu 6.06 LTS / 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : postfix vulnerability (USN-1131-1)
MEDIUM	5.0*	-	-	<a href="#">45037</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : apache2 vulnerabilities (USN-908-1)
MEDIUM	5.8*	-	-	<a href="#">45038</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : dpkg vulnerability (USN-909-1)
MEDIUM	5.0*	-	-	<a href="#">44108</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : expat vulnerability (USN-890-1)
MEDIUM	6.8*	-	-	<a href="#">44107</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : gzip vulnerability (USN-889-1)
MEDIUM	4.3*	-	-	<a href="#">42408</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : libhtml-parser vulnerability (USN-855-1)
MEDIUM	6.8*	-	-	<a href="#">45081</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-914-1)
MEDIUM	5.0*	-	-	<a href="#">43898</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : openssl vulnerability (USN-884-1)
MEDIUM	6.5*	-	-	<a href="#">43622</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerabilities (USN-876-1)



MEDIUM	4.4*	-	-	<a href="#">44336</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : samba vulnerability (USN-893-1)
MEDIUM	6.9*	-	-	<a href="#">44936</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : sudo vulnerability (USN-905-1)
MEDIUM	6.9*	-	-	<a href="#">45550</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : sudo vulnerability (USN-928-1)
MEDIUM	4.3*	-	-	<a href="#">40417</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : bind9 vulnerability (USN-808-1)
MEDIUM	4.6*	-	-	<a href="#">41624</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : newt vulnerability (USN-837-1)
MEDIUM	5.0*	-	-	<a href="#">39534</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : openssl vulnerabilities (USN-792-1)
MEDIUM	5.1*	-	-	<a href="#">40981</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : openssl vulnerability (USN-830-1)
MEDIUM	6.8*	-	-	<a href="#">41045</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : postgresql-8.1, postgresql-8.3 vulnerabilities (USN-834-1)
MEDIUM	6.8*	-	-	<a href="#">42050</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : wget vulnerability (USN-842-1)
MEDIUM	4.0*	-	-	<a href="#">37152</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : postgresql-8.1, postgresql-8.3 vulnerability (USN-753-1)
MEDIUM	5.8*	-	-	<a href="#">49644</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : apache2 vulnerability (USN-990-2)
MEDIUM	5.1*	-	-	<a href="#">49303</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : bzip2 vulnerability (USN-986-1)
MEDIUM	6.8*	-	-	<a href="#">47108</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : cups, cupswrapper vulnerabilities (USN-952-1)
MEDIUM	5.1*	-	-	<a href="#">49305</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : dpkg vulnerability (USN-986-3)
MEDIUM	6.8*	-	-	<a href="#">47778</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : freetype vulnerabilities (USN-963-1)
MEDIUM	6.8*	-	-	<a href="#">49066</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libwww-perl vulnerability (USN-981-1)

MEDIUM	4.6*	-	-	<a href="#">49791</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : lvm2 vulnerability (USN-1001-1)
MEDIUM	6.5*	-	-	<a href="#">46855</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : mysql-dfsg mysql-dfsg-5.1 vulnerabilities (USN-950-1)
MEDIUM	5.0*	-	-	<a href="#">48282</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : openldap openldap2.2, openldap2.3 vulnerabilities (USN-965-1)
MEDIUM	5.8*	-	-	<a href="#">49643</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : openssl vulnerability (USN-990-1)
MEDIUM	6.0*	-	-	<a href="#">49803</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : postgresql postgresql-8.3, postgresql-8.4 vulnerability (USN-1002-1)
MEDIUM	6.2*	-	-	<a href="#">47575</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : sudo vulnerability (USN-956-1)
MEDIUM	6.8*	-	-	<a href="#">47110</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : tiff vulnerabilities (USN-954-1)
MEDIUM	6.8*	-	-	<a href="#">48283</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : w3m vulnerability (USN-967-1)
MEDIUM	6.8*	-	-	<a href="#">49102</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : wget vulnerability (USN-982-1)
MEDIUM	6.5*	-	-	<a href="#">46179</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-933-1)
MEDIUM	5.0*	-	-	<a href="#">50823</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : apache2 vulnerabilities (USN-1021-1)
MEDIUM	4.3*	-	-	<a href="#">50560</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : libxml2 vulnerability (USN-1016-1)
MEDIUM	6.9*	-	-	<a href="#">50843</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : linux, linux-{ec2,source-2.6.15} vulnerabilities (USN-1023-1)
MEDIUM	5.0*	-	-	<a href="#">50573</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : mysql-5.0, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1017-1)
MEDIUM	4.3*	-	-	<a href="#">51076</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openssl vulnerabilities (USN-1029-1)
MEDIUM	5.0*	-	-	<a href="#">51525</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : php5 regression (USN-1042-2)

MEDIUM	6.8*	-	-	<a href="#">51502</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : php5 vulnerabilities (USN-1042-1)
MEDIUM	6.9*	-	-	<a href="#">55071</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : postfix vulnerabilities (USN-1113-1)
MEDIUM	6.5*	-	-	<a href="#">51871</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-1058-1)
MEDIUM	5.0*	-	-	<a href="#">52477</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : samba vulnerability (USN-1075-1)
MEDIUM	6.8*	-	-	<a href="#">53294</a>	Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff vulnerability (USN-1102-1)
MEDIUM	4.6*	-	-	<a href="#">57999</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : apache2 vulnerabilities (USN-1368-1)
MEDIUM	5.0*	-	-	<a href="#">56778</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : apache2, apache2-mpm-itk vulnerabilities (USN-1259-1)
MEDIUM	4.6*	-	-	<a href="#">57315</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : bzip2 vulnerability (USN-1308-1)
MEDIUM	5.0*	-	-	<a href="#">58618</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : gnutls13, gnutls26 vulnerabilities (USN-1418-1)
MEDIUM	6.8*	-	-	<a href="#">58443</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerability (USN-1402-1)
MEDIUM	6.8*	-	-	<a href="#">58617</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerability (USN-1417-1)
MEDIUM	5.0*	-	-	<a href="#">58145</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libxml2 vulnerability (USN-1376-1)
MEDIUM	6.9*	-	-	<a href="#">56629</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : pam vulnerabilities (USN-1237-1)
MEDIUM	6.4*	-	-	<a href="#">57314</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerability (USN-1307-1)
MEDIUM	6.8*	-	-	<a href="#">58168</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : postgresql-postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1378-1)
MEDIUM	6.8*	-	-	<a href="#">58600</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : tiff vulnerabilities (USN-1416-1)

MEDIUM	6.4*	-	-	<a href="#">57997</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : update-manager regression (USN-1284-2)
MEDIUM	6.8*	-	-	<a href="#">55699</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : libpng vulnerability (USN-1175-1)
MEDIUM	6.9*	-	-	<a href="#">55648</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : logrotate vulnerabilities (USN-1172-1)
MEDIUM	6.9*	-	-	<a href="#">55103</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : pam regression (USN-1140-2)
MEDIUM	6.9*	-	-	<a href="#">55102</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : pam vulnerability (USN-1140-1)
MEDIUM	5.0*	-	-	<a href="#">56506</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : postgresql-8.3, postgresql-8.4 vulnerability (USN-1229-1)
MEDIUM	6.9*	-	-	<a href="#">62434</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : dbus regressions (USN-1576-2)
MEDIUM	6.9*	-	-	<a href="#">62219</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : dbus vulnerability (USN-1576-1)
MEDIUM	6.8*	-	-	<a href="#">62388</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : eglibc vulnerabilities (USN-1589-1)
MEDIUM	5.0*	-	-	<a href="#">61485</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : expat vulnerabilities (USN-1527-1)
MEDIUM	5.0*	-	-	<a href="#">61706</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libgc vulnerability (USN-1546-1)
MEDIUM	5.0*	-	-	<a href="#">58974</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libtasn1 vulnerability (USN-1436-1)
MEDIUM	6.8*	-	-	<a href="#">59225</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libxml2 vulnerability (USN-1447-1)
MEDIUM	6.8*	-	-	<a href="#">62366</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libxml2 vulnerability (USN-1587-1)
MEDIUM	5.1*	-	-	<a href="#">59452</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : mysql-5.5, mysql-5.6, mysql-5.7 vulnerabilities (USN-1467-1)
MEDIUM	6.8*	-	-	<a href="#">59289</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : openssl vulnerabilities (USN-1451-1)

MEDIUM	4.3*	-	-	<a href="#">59385</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1461-1)
MEDIUM	4.9*	-	-	<a href="#">61607</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1542-1)
MEDIUM	6.8*	-	-	<a href="#">58872</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1427-1)
MEDIUM	5.0*	-	-	<a href="#">65607</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache vulnerabilities (USN-1765-1)
MEDIUM	5.0*	-	-	<a href="#">65981</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : curl vulnerability (USN-1801-1)
MEDIUM	4.3*	-	-	<a href="#">63536</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : freetype vulnerabilities (USN-1686-1)
MEDIUM	5.8*	-	-	<a href="#">63467</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : gnupg gnupg2 vulnerability (USN-1682-1)
MEDIUM	4.0*	-	-	<a href="#">64928</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : gnutls gnutls26 vulnerability (USN-1752-1)
MEDIUM	6.8*	-	-	<a href="#">63165</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libxml2 vulnerability (USN-1656-1)
MEDIUM	4.3*	-	-	<a href="#">65730</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libxml2 vulnerability (USN-1782-1)
MEDIUM	5.0*	-	-	<a href="#">64798</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : openssl vulnerabilities (USN-1732-1)
MEDIUM	6.8*	-	-	<a href="#">64616</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerability (USN-1717-1)
MEDIUM	6.9*	-	-	<a href="#">64969</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : sudo vulnerability (USN-1754-1)
MEDIUM	6.8*	-	-	<a href="#">62936</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : tiff vulnerabilities (USN-1631-1)
MEDIUM	6.8*	-	-	<a href="#">63164</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS : tiff vulnerability (USN-1655-1)
MEDIUM	6.9*	-	-	<a href="#">36749</a>	Ubuntu 8.04 LTS / 8.10 : dash vulnerability (USN-732-1)

MEDIUM	6.9*	-	-	<a href="#">38070</a>	Ubuntu 8.04 LTS / 8.10 : sudo vulnerability (USN-722-1)
MEDIUM	5.8*	-	-	<a href="#">47109</a>	Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : fastjar vulnerability (USN-953-1)
MEDIUM	5.0*	-	-	<a href="#">50824</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : apr-util vulnerability (USN-1022-1)
MEDIUM	5.8*	-	-	<a href="#">51583</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : fuse vulnerability (USN-1045-1)
MEDIUM	6.8*	-	-	<a href="#">53257</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openldap, openldap vulnerabilities (USN-1100-1)
MEDIUM	5.8*	-	-	<a href="#">51584</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : util-linux update (USN-1045-2)
MEDIUM	6.8*	-	-	<a href="#">63285</a>	Ubuntu 8.04 LTS : glibc regression (USN-1589-2)
MEDIUM	6.9*	-	-	<a href="#">55784</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1186-1)
MEDIUM	5.4*	-	-	<a href="#">57495</a>	Ubuntu 8.04 LTS : linux vulnerabilities (USN-1323-1)
MEDIUM	4.9*	-	-	<a href="#">59292</a>	Ubuntu 8.04 LTS : linux vulnerability (USN-1454-1)
MEDIUM	4.7*	-	-	<a href="#">63122</a>	Ubuntu 8.04 LTS : linux vulnerability (USN-1650-1)
MEDIUM	5.0*	-	-	<a href="#">63221</a>	Ubuntu 8.04 LTS : linux vulnerability (USN-1660-1)
MEDIUM	4.3*	-	-	<a href="#">33389</a>	Ubuntu 8.04 LTS : openssl vulnerabilities (USN-620-1)
MEDIUM	6.9*	-	-	<a href="#">62619</a>	Ubuntu 8.04 LTS : python2.5 vulnerabilities (USN-1613-1)
LOW	5.9	-	-	<a href="#">31705</a>	SSL Anonymous Cipher Suites Supported
LOW	3.7	-	-	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	-	-	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	-	-	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	2.1*	-	-	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled

LOW	3.3*	-	-	<a href="#">44335</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : fuse vulnerability (USN-892-1)
LOW	3.5*	-	-	<a href="#">45343</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : samba vulnerability (USN-918-1)
LOW	3.6*	-	-	<a href="#">39786</a>	Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dbus vulnerability (USN-799-1)
LOW	2.1*	-	-	<a href="#">36904</a>	Ubuntu 7.10 / 8.04 LTS : postfix vulnerability (USN-642-1)
LOW	2.6*	-	-	<a href="#">56970</a>	Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apt vulnerability (USN-1283-1)
LOW	2.6*	-	-	<a href="#">59554</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : apt vulnerability (USN-1477-1)
LOW	2.6*	-	-	<a href="#">62869</a>	Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache vulnerabilities (USN-1627-1)
LOW	2.1*	-	-	<a href="#">51572</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : dbus vulnerability (USN-1044-1)
LOW	3.3*	-	-	<a href="#">52479</a>	Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : fuse vulnerabilities (USN-1077-1)
LOW	2.6*	-	-	<a href="#">10407</a>	X Server Detection
INFO	N/A	-	-	<a href="#">10223</a>	RPC portmapper Service Detection
INFO	N/A	-	-	<a href="#">21186</a>	AJP Connector Detection
INFO	N/A	-	-	<a href="#">18261</a>	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	<a href="#">141394</a>	Apache HTTP Server Installed (Linux)
INFO	N/A	-	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	-	<a href="#">156000</a>	Apache Log4j Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">39446</a>	Apache Tomcat Detection
INFO	N/A	-	-	<a href="#">34098</a>	BIOS Info (SSH)
INFO	N/A	-	-	<a href="#">39519</a>	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	<a href="#">84574</a>	Backported Security Patch Detection (PHP)
INFO	N/A	-	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)

INFO	N/A	-	-	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	-	<a href="#">182774</a>	Curl Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">10028</a>	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	<a href="#">35373</a>	DNS Server DNSSEC Aware Resolver
INFO	N/A	-	-	<a href="#">11002</a>	DNS Server Detection
INFO	N/A	-	-	<a href="#">72779</a>	DNS Server Version Detection
INFO	N/A	-	-	<a href="#">35371</a>	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	<a href="#">55472</a>	Device Hostname
INFO	N/A	-	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	-	<a href="#">25203</a>	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	-	<a href="#">25202</a>	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	-	<a href="#">33276</a>	Enumerate MAC Addresses via SSH
INFO	N/A	-	-	<a href="#">170170</a>	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	-	<a href="#">179200</a>	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	-	<a href="#">168980</a>	Enumerate the PATH Variables
INFO	N/A	-	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	-	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	-	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	<a href="#">171410</a>	IP Assignment Method Detection
INFO	N/A	-	-	<a href="#">157358</a>	Linux Mounted Devices
INFO	N/A	-	-	<a href="#">193143</a>	Linux Time Zone Information
INFO	N/A	-	-	<a href="#">95928</a>	Linux User List Enumeration



INFO	N/A	-	-	<a href="#">10397</a>	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	<a href="#">10719</a>	MySQL Server Detection
INFO	N/A	-	-	<a href="#">10437</a>	NFS Share Export List
INFO	N/A	-	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	-	<a href="#">64582</a>	Netstat Connection Information
INFO	N/A	-	-	<a href="#">14272</a>	Netstat Portscanner (SSH)
INFO	N/A	-	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	-	<a href="#">97993</a>	OS Identification and Installed Software Enumeration over SSH (Using New SSH Library)
INFO	N/A	-	-	<a href="#">117887</a>	OS Security Patch Assessment Available
INFO	N/A	-	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	-	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	-	-	<a href="#">168007</a>	OpenSSL Installed (Linux)
INFO	N/A	-	-	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	-	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	-	<a href="#">130024</a>	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	-	<a href="#">118224</a>	PostgreSQL STARTTLS Support
INFO	N/A	-	-	<a href="#">26024</a>	PostgreSQL Server Detection
INFO	N/A	-	-	<a href="#">22227</a>	RMI Registry Detection
INFO	N/A	-	-	<a href="#">11111</a>	RPC Services Enumeration
INFO	N/A	-	-	<a href="#">53335</a>	RPC portmapper (TCP)

INFO	N/A	-	-	<a href="#">45405</a>	Reachable IPv6 address
INFO	N/A	-	-	<a href="#">202184</a>	Ruby Programming Language Installed (Linux)
INFO	N/A	-	-	<a href="#">10263</a>	SMTP Server Detection
INFO	N/A	-	-	<a href="#">42088</a>	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	-	<a href="#">102094</a>	SSH Commands Require Privilege Escalation
INFO	N/A	-	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	-	<a href="#">90707</a>	SSH SCP Protocol Detection
INFO	N/A	-	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	-	<a href="#">45410</a>	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	-	<a href="#">62563</a>	SSL Compression Methods Supported
INFO	N/A	-	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	<a href="#">51891</a>	SSL Session Resume Supported
INFO	N/A	-	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	-	<a href="#">104887</a>	Samba Version
INFO	N/A	-	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	-	<a href="#">11153</a>	Service Detection (HELP Request)

INFO	N/A	-	-	<a href="#">22869</a>	Software Enumeration (SSH)
INFO	N/A	-	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	-	<a href="#">11819</a>	TFTP Daemon Detection
INFO	N/A	-	-	<a href="#">110385</a>	Target Credential Issues by Authentication Protocol - Insufficient Privilege
INFO	N/A	-	-	<a href="#">141118</a>	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	-	<a href="#">10281</a>	Telnet Server Detection
INFO	N/A	-	-	<a href="#">56468</a>	Time of Last System Startup
INFO	N/A	-	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	-	<a href="#">110483</a>	Unix / Linux Running Processes Information
INFO	N/A	-	-	<a href="#">152742</a>	Unix Software Discovery Commands Available
INFO	N/A	-	-	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	<a href="#">19288</a>	VNC Server Security Type Detection
INFO	N/A	-	-	<a href="#">65792</a>	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	<a href="#">10342</a>	VNC Software Detection
INFO	N/A	-	-	<a href="#">189731</a>	Vim Installed (Linux)
INFO	N/A	-	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	-	<a href="#">20108</a>	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	<a href="#">11422</a>	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	-	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	-	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	<a href="#">182848</a>	libcurl Installed (Linux / Unix)
INFO	N/A	-	-	<a href="#">52703</a>	vsftpd Detection

\* indicates the v3.0 score was not available; the v2.0 score is shown