



OUTSCAN Security Report

Sections

[Report info >>](#)

[Delta host overview >>](#)

[Vulnerability details >>](#)

[Scan tracking list >>](#)

Report info

Report Type:	Delta report
Report ID:	9805A21CB2BA65F6B11C6D6D8846B0AC
Date Report was created:	2010-03-17 05:58
Timezone for dates:	GMT
Report created for:	Demo company
Schedule job:	All europe
IPs:	intra.example.com - 192.168.200.45
Scanning interval:	2009-11-17 10:57 - 2009-11-17 11:33
Number of Findings found:	64
Number of Accepted Risks:	1

Delta host overview

	Added	Unchanged	Removed
intra.example.com - 192.168.200.45	41	10	13

Vulnerability details - 192.168.200.45 (intra.example.com)

Script ID:	110956
Name:	Anonymous SMB Login Enabled
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	7.5 - (AV:N/AC:L/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	generic
Description:	Anonymous access to this SMB service is enabled. If this is an internet-facing server, having anonymous access to it is generally a bad idea.
Solution:	Reconfigure this service.
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	113289
Name:	NetBIOS Name Enumeration
Port:	137/udp - netbios-ns

Family:	smb																	
Description:	A NetBIOS service replies to queries on udp port 137.																	
Information:	MAC address: 00:00:00:00:00:00 (Probably a SAMBA server)																	
	NetBIOS names found:																	
	<table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>UBUNTU810</td> <td>computer name</td> </tr> <tr> <td>UBUNTU810</td> <td>messenger service</td> </tr> <tr> <td>UBUNTU810</td> <td>file server service</td> </tr> <tr> <td>__MSBROWSE__</td> <td>master browser</td> </tr> <tr> <td>WORKGROUP</td> <td>master browser</td> </tr> <tr> <td>WORKGROUP</td> <td>browser service elections</td> </tr> <tr> <td>WORKGROUP</td> <td>workgroup / domain name</td> </tr> </tbody> </table>	Name	Description	UBUNTU810	computer name	UBUNTU810	messenger service	UBUNTU810	file server service	__MSBROWSE__	master browser	WORKGROUP	master browser	WORKGROUP	browser service elections	WORKGROUP	workgroup / domain name	
Name	Description																	
UBUNTU810	computer name																	
UBUNTU810	messenger service																	
UBUNTU810	file server service																	
__MSBROWSE__	master browser																	
WORKGROUP	master browser																	
WORKGROUP	browser service elections																	
WORKGROUP	workgroup / domain name																	
CVE:	CVE-1999-0621																	
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57																	
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57																	

Script ID:	124463
Name:	HTTP Detection
Port:	8080/tcp - http
Family:	http
Description:	An HTTP server was found running on the remote host.
Information:	Apache-Coyote/1.1
Virtual host:	192.168.200.45
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	125644			
Name:	SMB Network Share Enumeration			
Port:	445/tcp - netbios-ssn			
Family:	smb			
Description:	SMB shares available on this host:			
Information:	<table border="1"> <thead> <tr> <th>Share name</th> </tr> </thead> <tbody> <tr> <td>print\$</td> </tr> <tr> <td>IPC\$</td> </tr> </tbody> </table>	Share name	print\$	IPC\$
Share name				
print\$				
IPC\$				
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding			
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22			

Script ID:	125665
Name:	SMB LanMan Pipe Server Browsing
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	This host will reveal the list of other nearby Windows systems when queried through the LanMan pipe.
Information:	The following hosts were revealed: UBUNTU810 (os version: 0.0)
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	125677
Name:	SMB Native LanMan Information
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	Sending an authentication request to this host reveals the following information:
Information:	Domain: UBUNTU810 Native LanMan: Samba 3.2.3 Operating System: Unix
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	125796
Name:	SMB Host Password Policy
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	The remote host has a password policy set. This password policy must conform to the International System Policy.
Information:	Note: OUTSCAN used the supplied credentials to authenticate The remote host has the following password policy: Password history length: 0 Minimum password length: 5 Password aging: 0 days Password complexity requirements: Enabled Minimum password age: 0 days Forced logoff: Disabled Locked account after: 1800 seconds Time between failed logons: 1800 seconds
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	125898
Name:	SSH Banner
Port:	22/tcp - ssh
Family:	ssh
Description:	The SSH server banner:
Information:	SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	125901
Name:	SSH Supported Protocol Versions
Port:	22/tcp - ssh
Family:	ssh
Description:	The remote host is running a version of the SSH protocol. OUTSCAN has detected that the following is true for the remote host.
Information:	The SSH service appears to support the protocol version(s): 1.99, 2.0 Hostkey version 2: 33:8f:7c:a6:11:c0:25:5f:1f:f1:8b:ad:18:fb:09:84
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	125950
Name:	TCP SYN FIN
Port:	General
Family:	low level network testing
Description:	<p>The TCP implementation on this host replies to invalid TCP packets. Packets with both the SYN and the FIN bit set are considered invalid and should be discarded.</p> <p>Not doing so could have a negative impact on IDS systems. Depending on the order in which the flag-bits are parsed, the TCP implementation of this host's operating system may see the SYN bit first and initiate a connection while the TCP implementation of the IDS parses the FIN bit first, making it believe that the connection has just been closed.</p> <p>Effectively, this could mean that a connection can be established without the IDS keeping track of it.</p>
Solution:	Contact your operating system vendor for a patch.
Reference:	url - http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html url - http://www.kb.cert.org/vuls/id/464113 url - http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-3537
Bugtraq:	7487

History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	125993
Name:	Traceroute
Port:	General
Family:	misc
Description:	<p>This check tries to determine the path; traceroute, between our attacker and your target host. This path may give an attacker valuable information about through which routers; hops, traffic passes through. This is not a vulnerability in itself it is merely considered information, however, an attacker could possibly use this information to determine what ISP you have and so forth.</p> <p>Note: The path is not static and will most likely change depending on from which host you perform the traceroute. There is also no way you can fix this problem as it involves changing configurations on all the hops along the way.</p>
Information:	<pre>host[:dport]/protocol (1 hops) 1 192.168.200.45:53/udp [closed]</pre>
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	200217
Name:	ICMP Timestamp Request
Port:	General
Family:	low level network testing
Description:	<p>The remote host replies to ICMP Timestamp requests.</p> <p>Knowing the exact time on your system may help an attacker to break time-based authentication systems.</p>
Solution:	Filter incoming ICMP type 13, and outgoing ICMP type 14 packets.
CVE:	CVE-1999-0524
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	200275
Name:	SMB Host Security Identifier
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	It was possible to get the host Security Identifier (SID) through the SMB service, by calling LsaQueryInformationPolicy. This can be used to enumerate local user accounts.

Information:	SID: 1-5-21-897084493--634054598--2011538493
Solution:	Restrict access to the SMB service
CVE:	CVE-2000-1200
Bugtraq:	959
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	200276
Name:	SMB Host SID Local User Enumeration
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	It was possible to enumerate the local users of the remote host. This could give an attacker valuable information.
Information:	The following accounts were found during the enumeration: Guest account name: nobody
CVE:	CVE-2000-1200
Bugtraq:	959
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	200823
Name:	SSH Supported Authentication Mechanisms
Port:	22/tcp - ssh
Family:	ssh
Description:	The SSH service running on this port supports the following authentication mechanisms.
Information:	publickey,password
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	200825
Name:	HTTP Options Supported
Port:	8080/tcp - http
Family:	http
Description:	The following options are supported by the web server running on this port.

Information:	GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Virtual host:	192.168.200.45
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	200826		
Name:	HTTP Information		
Port:	8080/tcp - http		
Family:	http		
Description:	HTTP Server Information		
Information:	<u>HTTP Version</u> 1.1	<u>SSL</u> no	<u>Request Pipelining</u> yes
			<u>Connection Keep-Alive</u> yes
Reference:	url - http://www.mozilla.org/projects/netlib/http/pipelining-faq.html url - http://www.io.com/~maus/HttpKeepAlive.html		
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-17 10:57		
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57		

Script ID:	215073
Name:	Samba: smbd *trans* Request Arbitrary Remote Memory Disclosure
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	8.5 - (AV:N/AC:L/Au:N/C:C/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba
Description:	smbd in Samba might allow remote attackers to read arbitrary memory and cause a denial of service via crafted (1) trans, (2) trans2, and (3) ntrans requests, related to a "cut&paste error" that causes an improper bounds check to be performed.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is greater than or equal to 3.0.29; and (2) the version of Samba, 3.2.3, is less than or equal to 3.2.4.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2008-4314
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	217011
Name:	Samba Root Filesystem Access Vulnerability
Port:	445/tcp - netbios-ssn

Risk factor:	Medium risk
CVSS Score:	6.3 - (AV:N/AC:M/Au:S/C:C/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba
Description:	Samba 3.2.0 through 3.2.6, when registry shares are enabled, allows remote authenticated users to access the root filesystem via a crafted connection request that specifies a blank share name.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is greater than or equal to 3.2.0; and (2) the version of Samba, 3.2.3, is less than or equal to 3.2.6.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2009-0022
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	217925
Name:	SMB Login
Port:	445/tcp - netbios-ssn
Family:	smb
Description:	This check attempts to login to the remote SMB service.
Information:	The following login attempts were successful: - Null session [<blank> / <blank>] - Anonymous login [<random> / <random>] Selected login type: Anonymous login
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	217926
Name:	SMB Null Sessions Enabled
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	7.5 - (AV:N/AC:L/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	generic
Description:	This SMB service accepts anonymous connections in the form of Null sessions. If this is an internet-facing server, having anonymous access to it is generally a bad idea.
Solution:	Reconfigure this service.
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	219054
Name:	Samba: POSIX Access Control Override
Port:	445/tcp - netbios-ssn
Risk factor:	Medium risk
CVSS Score:	5.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba
Description:	The acl_group_override function in smbd/posix_acls.c in smbd in Samba 3.0.x before 3.0.35, 3.1.x and 3.2.x before 3.2.13, and 3.3.x before 3.3.6, when dos filemode is enabled, allows remote attackers to modify access control lists for files via vectors related to read access to uninitialized memory.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is less than or equal to 3.2.12.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2009-1888
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	219055
Name:	Samba: Filename-base Format String Bug
Port:	445/tcp - netbios-ssn
Risk factor:	High risk
CVSS Score:	9.3 - (AV:N/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	samba
Description:	Multiple format string vulnerabilities in client/client.c in smbclient in Samba 3.2.0 through 3.2.12 might allow context-dependent attackers to execute arbitrary code via format string specifiers in a filename.
Information:	This vulnerability was identified because (1) the version of Samba, 3.2.3, is less than or equal to 3.2.12.
Solution:	Upgrade to the latest version of Samba
CVE:	CVE-2009-1886
History:	First Seen : 2009-11-06 13:22 - Last Seen : 2009-11-06 13:22 - Fixed Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-03 13:22

Script ID:	230324
Name:	USN-673-1: libxml2 vulnerabilities
Port:	22/tcp - ssh
Risk factor:	High risk
CVSS Score:	7.8 - (AV:N/AC:L/Au:N/C:N/I:N/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu

Description:	Integer overflow in the xmlBufferResize function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of service (infinite loop) via a large XML document.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'libxml2' Ubuntu package, 2.6.32.dfsg-4ubuntu1, is less than 2.6.32.dfsg-4ubuntu1.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-673-1
CVE:	CVE-2008-4225
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230325 - Marked as false positive
Name:	USN-673-1: libxml2 vulnerabilities
Port:	22/tcp - ssh
Risk factor:	High risk
CVSS Score:	10.0 - (AV:N/AC:L/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Integer overflow in the xmlSAX2Characters function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a large XML document.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'libxml2' Ubuntu package, 2.6.32.dfsg-4ubuntu1, is less than 2.6.32.dfsg-4ubuntu1.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-673-1
CVE:	CVE-2008-4226
History:	First Seen : 2009-11-06 14:45 - New Finding Risk Accepted : 2010-02-23 08:56 Acceptance Expires : 2010-03-25 08:56 Accepted By : Demo Account
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230354
Name:	USN-680-1: Samba vulnerability
Port:	22/tcp - ssh
Risk factor:	High risk
CVSS Score:	8.5 - (AV:N/AC:L/Au:N/C:C/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	smbd in Samba 3.0.29 through 3.2.4 might allow remote attackers to read arbitrary memory and cause a denial of service via crafted (1) trans, (2) trans2, and (3) ntrans requests, related to a "cut&paste error"

	denial of service via crafted (1) trans, (2) trans2, and (3) nttrans requests, related to a "cut&paste error" that causes an improper bounds check to be performed.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'samba' Ubuntu package, 2:3.2.3-1ubuntu3, is less than 2:3.2.3-1ubuntu3.3.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-680-1
CVE:	CVE-2008-4314
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230411
Name:	USN-700-1: Perl vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Directory traversal vulnerability in the Archive::Tar Perl module 1.36 and earlier allows user-assisted remote attackers to overwrite arbitrary files via a TAR archive that contains a file whose name is an absolute path or has ".." sequences.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'perl' Ubuntu package, 5.10.0-11.1ubuntu2, is less than 5.10.0-11.1ubuntu2.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-700-1
CVE:	CVE-2007-4829
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230413
Name:	USN-700-1: Perl vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.9 - (AV:L/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Race condition in the rmtree function in File::Path 1.08 and 2.07 (lib/File/Path.pm) in Perl 5.8.8 and 5.10.0 allows local users to create arbitrary setuid binaries via a symlink attack, a different vulnerability than CVE-2005-0448, CVE-2004-0452, and CVE-2008-2827. NOTE: this is a regression error related to CVE-2005-0448. It is different from CVE-2008-5303 due to affected versions.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'perl' Ubuntu package, 5.10.0-11.1ubuntu2, is less than 5.10.0-11.1ubuntu2.2.

and (2) the version of the 'perl' Ubuntu package, 5.10.0-11.1ubuntu2, is less than 5.10.0-11.1ubuntu2.2.

Solution: Upgrade to the latest version of Ubuntu

Reference: solution - <http://www.ubuntu.com/usn/USN-700-1>

CVE: CVE-2008-5302

History: First Seen : 2009-11-06 14:45 - **New Finding**

Target: intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID: 230415

Name: USN-700-2: Perl regression

Port: 22/tcp - ssh

Risk factor: Medium risk

CVSS Score: 6.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

Family: ubuntu

Description: Directory traversal vulnerability in the Archive::Tar Perl module 1.36 and earlier allows user-assisted remote attackers to overwrite arbitrary files via a TAR archive that contains a file whose name is an absolute path or has ".." sequences.

Information: This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'perl' Ubuntu package, 5.10.0-11.1ubuntu2, is less than 5.10.0-11.1ubuntu2.2.

Solution: Upgrade to the latest version of Ubuntu

Reference: solution - <http://www.ubuntu.com/usn/USN-700-2>

CVE: CVE-2007-4829

History: First Seen : 2009-11-06 14:45 - **New Finding**

Target: intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID: 230417

Name: USN-700-2: Perl regression

Port: 22/tcp - ssh

Risk factor: Medium risk

CVSS Score: 6.9 - (AV:L/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

Family: ubuntu

Description: Race condition in the rmtree function in File::Path 1.08 and 2.07 (lib/File/Path.pm) in Perl 5.8.8 and 5.10.0 allows local users to create arbitrary setuid binaries via a symlink attack, a different vulnerability than CVE-2005-0448, CVE-2004-0452, and CVE-2008-2827. NOTE: this is a regression error related to CVE-2005-0448. It is different from CVE-2008-5303 due to affected versions.

Information: This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'perl' Ubuntu package, 5.10.0-11.1ubuntu2, is less than 5.10.0-11.1ubuntu2.2.

Solution: Upgrade to the latest version of Ubuntu

Reference:	solution - http://www.ubuntu.com/usn/USN-700-2
CVE:	CVE-2008-5302
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230434
Name:	USN-702-1: Samba vulnerability
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.3 - (AV:N/AC:M/Au:S/C:C/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Samba 3.2.0 through 3.2.6, when registry shares are enabled, allows remote authenticated users to access the root filesystem via a crafted connection request that specifies a blank share name.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'samba' Ubuntu package, 2:3.2.3-1ubuntu3, is less than 2:3.2.3-1ubuntu3.4.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-702-1
CVE:	CVE-2009-0022
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230438
Name:	USN-704-1: OpenSSL vulnerability
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.8 - (AV:N/AC:M/Au:N/C:N/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-704-1
CVE:	CVE-2008-5077
History:	First Seen : 2009-11-06 14:45 - New Finding

Target: intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID: 230516

Name: USN-722-1: sudo vulnerability

Port: 22/tcp - ssh

Risk factor: Medium risk

CVSS Score: 6.9 - (AV:L/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

Family: ubuntu

Description: parse.c in sudo 1.6.9p17 through 1.6.9p19 does not properly interpret a system group (aka %group) in the sudoers file during authorization decisions for a user who belongs to that group, which allows local users to leverage an applicable sudoers file and gain root privileges via a sudo command.

Information: This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'sudo' Ubuntu package, 1.6.9p17-1ubuntu2, is less than 1.6.9p17-1ubuntu2.1.

Solution: Upgrade to the latest version of Ubuntu

Reference: solution - <http://www.ubuntu.com/usn/USN-722-1>

CVE: CVE-2009-0034

History: First Seen : 2009-11-06 14:45 - **New Finding**

Target: intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID: 230553

Name: USN-732-1: dash vulnerability

Port: 22/tcp - ssh

Risk factor: Medium risk

CVSS Score: 6.9 - (AV:L/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

Family: ubuntu

Description: Untrusted search path vulnerability in dash 0.5.4, when used as a login shell, allows local users to execute arbitrary code via a Trojan horse .profile file in the current working directory.

Information: This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'dash' Ubuntu package, 0.5.4-9ubuntu1, is less than 0.5.4-9ubuntu1.1.

Solution: Upgrade to the latest version of Ubuntu

Reference: solution - <http://www.ubuntu.com/usn/USN-732-1>

CVE: CVE-2009-0854

History: First Seen : 2009-11-06 14:45 - **New Finding**

Target: intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID: 230596

Name:	USN-750-1: OpenSSL vulnerability
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-750-1
CVE:	CVE-2009-0590
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230639
Name:	USN-758-1: udev vulnerabilities
Port:	22/tcp - ssh
Risk factor:	High risk
CVSS Score:	7.1 - (AV:L/AC:L/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	udev before 1.4.1 does not verify whether a NETLINK message originates from kernel space, which allows local users to gain privileges by sending a NETLINK message from user space.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'udev' Ubuntu package, 124-8, is less than 124-9ubuntu0.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-758-1
CVE:	CVE-2009-1185
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230640
Name:	USN-758-1: udev vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Low risk

CVSS Score:	2.1 - (AV:L/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Buffer overflow in the util_path_encode function in udev/lib/libudev-util.c in udev before 1.4.1 allows local users to cause a denial of service (service outage) via vectors that trigger a call with crafted arguments.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'udev' Ubuntu package, 124-8, is less than 124-9ubuntu0.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-758-1
CVE:	CVE-2009-1186
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230659
Name:	USN-762-1: APT vulnerabilities
Port:	22/tcp - ssh
Risk factor:	High risk
CVSS Score:	10.0 - (AV:N/AC:L/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	apt 0.7.20 does not check when the date command returns an "invalid date" error, which can prevent apt from loading security updates in time zones for which DST occurs at midnight.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'apt' Ubuntu package, 0.7.14ubuntu6, is less than 0.7.14ubuntu6.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-762-1
CVE:	CVE-2009-1300
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230697
Name:	USN-778-1: cron vulnerability
Port:	22/tcp - ssh
Risk factor:	High risk
CVSS Score:	7.1 - (AV:L/AC:L/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	do_command.c in Vixie cron (vixie-cron) 4.1 does not check the return code of a setuid call, which might allow local users to gain root privileges if setuid fails in cases such as PAM failures or resource limits, as originally demonstrated by a program that exceeds the process limits as defined in

	originally demonstrated by a program that exceeds the process limits as defined in /etc/security/limits.conf.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'cron' Ubuntu package, 3.0p1-104+ubuntu5, is less than 3.0p1-104+ubuntu5.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-778-1
CVE:	CVE-2006-2607
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230739
Name:	USN-788-1: Tomcat vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:P/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, 6.0.0 through 6.0.18, and possibly earlier versions normalizes the target pathname before filtering the query string when using the RequestDispatcher method, which allows remote attackers to bypass intended access restrictions and conduct directory traversal attacks via .. (dot dot) sequences and the WEB-INF directory in a Request.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'tomcat6' Ubuntu package, 6.0.18-0ubuntu3, is less than 6.0.18-0ubuntu3.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-788-1
CVE:	CVE-2008-5515
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230740
Name:	USN-788-1: Tomcat vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18, when the Java AJP connector and mod_jk load balancing are used, allows remote attackers to cause a denial of service (application outage) via a crafted request with invalid headers, related to temporary blocking of connectors that have encountered errors, as demonstrated by an error involving a malformed HTTP Host header.

	Host header.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'tomcat6' Ubuntu package, 6.0.18-0ubuntu3, is less than 6.0.18-0ubuntu3.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-788-1
CVE:	CVE-2009-0033
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230741
Name:	USN-788-1: Tomcat vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	4.3 - (AV:N/AC:M/Au:N/C:P/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18, when FORM authentication is used, allows remote attackers to enumerate valid usernames via requests to <code>/j_security_check</code> with malformed URL encoding of passwords, related to improper error checking in the (1) MemoryRealm, (2) DataSourceRealm, and (3) JDBCRealm authentication realms, as demonstrated by a % (percent) value for the <code>j_password</code> parameter.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'tomcat6' Ubuntu package, 6.0.18-0ubuntu3, is less than 6.0.18-0ubuntu3.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-788-1
CVE:	CVE-2009-0580
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230742
Name:	USN-788-1: Tomcat vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	4.3 - (AV:N/AC:M/Au:N/C:N/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Cross-site scripting (XSS) vulnerability in <code>jsp/cal/cal2.jsp</code> in the calendar application in the examples web application in Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 allows remote attackers to inject arbitrary web script or HTML via the time parameter, related to "invalid HTML."

Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'tomcat6' Ubuntu package, 6.0.18-0ubuntu3, is less than 6.0.18-0ubuntu3.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-788-1
CVE:	CVE-2009-0781
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230743
Name:	USN-788-1: Tomcat vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Low risk
CVSS Score:	3.6 - (AV:L/AC:L/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 permits web applications to replace an XML parser used for other web applications, which allows local users to read or modify the (1) web.xml, (2) context.xml, or (3) tld files of arbitrary web applications via a crafted application that is loaded earlier than the target application.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'tomcat6' Ubuntu package, 6.0.18-0ubuntu3, is less than 6.0.18-0ubuntu3.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-788-1
CVE:	CVE-2009-0783
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230762
Name:	USN-792-1: OpenSSL vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.4.

Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-792-1
CVE:	CVE-2009-1377
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230763
Name:	USN-792-1: OpenSSL vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.4.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-792-1
CVE:	CVE-2009-1378
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230764
Name:	USN-792-1: OpenSSL vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Use-after-free vulnerability in the dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL 1.0.0 Beta 2 allows remote attackers to cause a denial of service (openssl s_client crash) and possibly have unspecified other impact via a DTLS packet, as demonstrated by a packet from a server that uses a crafted server certificate.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.4.
Solution:	Upgrade to the latest version of Ubuntu

Reference:	solution - http://www.ubuntu.com/usn/USN-792-1
CVE:	CVE-2009-1379
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230765
Name:	USN-792-1: OpenSSL vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	ssl/s3_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.4.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-792-1
CVE:	CVE-2009-1386
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230766
Name:	USN-792-1: OpenSSL vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	5.0 - (AV:N/AC:L/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a "fragment bug."
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.4.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-792-1
CVE:	CVE-2009-1387

History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230782
Name:	USN-794-1: Perl vulnerability
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Off-by-one error in the inflate function in Zlib.xs in Compress::Raw::Zlib Perl module before 2.017, as used in AMaViS, SpamAssassin, and possibly other products, allows context-dependent attackers to cause a denial of service (hang or crash) via a crafted zlib compressed stream that triggers a heap-based buffer overflow, as exploited in the wild by Trojan.Downloader-71014 in June 2009.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 9.04.*; and (2) the version of the 'libcompress-raw-zlib-perl' Ubuntu package, 2.011-2build1, is less than 2.015-1ubuntu0.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-794-1
CVE:	CVE-2009-1391
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230794
Name:	USN-799-1: D-Bus vulnerability
Port:	22/tcp - ssh
Risk factor:	Low risk
CVSS Score:	3.6 - (AV:L/AC:L/Au:N/C:N/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The _dbus_validate_signature_with_reason function (dbus-marshal-validate.c) in D-Bus (aka DBus) before 1.2.14 uses incorrect logic to validate a basic type, which allows remote attackers to spoof a signature via a crafted key. NOTE: this is due to an incorrect fix for CVE-2008-3834.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'dbus' Ubuntu package, 1.2.4-0ubuntu1, is less than 1.2.4-0ubuntu1.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-799-1
CVE:	CVE-2009-1189
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230814
Name:	USN-809-1: GnuTLS vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.4 - (AV:N/AC:L/Au:N/C:N/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.5.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-809-1
CVE:	CVE-2009-2409
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230818
Name:	USN-810-1: NSS vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.4 - (AV:N/AC:L/Au:N/C:N/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.5.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-810-1
CVE:	CVE-2009-2409
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230821
Name:	USN-810-2: NSPR update
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.4 - (AV:N/AC:L/Au:N/C:N/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.5.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-810-2
CVE:	CVE-2009-2409
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230824
Name:	USN-810-3: NSS regression
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.4 - (AV:N/AC:L/Au:N/C:N/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.5.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-810-3
CVE:	CVE-2009-2409
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230845
Name:	USN-815-1: libxml2 vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	4.3 - (AV:N/AC:M/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Stack consumption vulnerability in libxml2 2.5.10, 2.6.16, 2.6.26, 2.6.27, and 2.6.32, and libxml 1.8.17, allows context-dependent attackers to cause a denial of service (application crash) via a large depth of element declarations in a DTD, related to a function recursion, as demonstrated by the Codenomicon XML fuzzing framework.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'libxml2' Ubuntu package, 2.6.32.dfsg-4ubuntu1, is less than 2.6.32.dfsg-4ubuntu1.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-815-1
CVE:	CVE-2009-2414
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230846
Name:	USN-815-1: libxml2 vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	4.3 - (AV:N/AC:M/Au:N/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Multiple use-after-free vulnerabilities in libxml2 2.5.10, 2.6.16, 2.6.26, 2.6.27, and 2.6.32, and libxml 1.8.17, allow context-dependent attackers to cause a denial of service (application crash) via crafted (1) Notation or (2) Enumeration attribute types in an XML file, as demonstrated by the Codenomicon XML fuzzing framework.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'libxml2' Ubuntu package, 2.6.32.dfsg-4ubuntu1, is less than 2.6.32.dfsg-4ubuntu1.2.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-815-1
CVE:	CVE-2009-2416
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230876
-------------------	--------

Name:	USN-830-1: OpenSSL vulnerability
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.4 - (AV:N/AC:L/Au:N/C:N/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The Network Security Services (NSS) library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'openssl' Ubuntu package, 0.9.8g-10.1ubuntu2, is less than 0.9.8g-10.1ubuntu2.5.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-830-1
CVE:	CVE-2009-2409
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230900
Name:	USN-839-1: Samba vulnerabilities
Port:	22/tcp - ssh
Risk factor:	High risk
CVSS Score:	9.3 - (AV:N/AC:M/Au:N/C:C/I:C/A:C) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Multiple format string vulnerabilities in client/client.c in smbclient in Samba 3.2.0 through 3.2.12 might allow context-dependent attackers to execute arbitrary code via format string specifiers in a filename.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'samba' Ubuntu package, 2:3.2.3-1ubuntu3, is less than 2:3.2.3-1ubuntu3.6.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-839-1
CVE:	CVE-2009-1886
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230901
Name:	USN-839-1: Samba vulnerabilities
Port:	22/tcp - ssh

Risk factor:	Medium risk
CVSS Score:	5.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	The acl_group_override function in smbd/posix_acls.c in smbd in Samba 3.0.x before 3.0.35, 3.1.x and 3.2.x before 3.2.13, and 3.3.x before 3.3.6, when dos filemode is enabled, allows remote attackers to modify access control lists for files via vectors related to read access to uninitialized memory.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'samba' Ubuntu package, 2:3.2.3-1ubuntu3, is less than 2:3.2.3-1ubuntu3.6.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-839-1
CVE:	CVE-2009-1888
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230902
Name:	USN-839-1: Samba vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.0 - (AV:N/AC:M/Au:S/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	Samba 3.4 before 3.4.2, 3.3 before 3.3.8, 3.2 before 3.2.15, and 3.0.12 through 3.0.36, as used in the SMB subsystem in Apple Mac OS X 10.5.8 when Windows File Sharing is enabled, Fedora 11, and other operating systems, does not properly handle errors in resolving pathnames, which allows remote authenticated users to bypass intended sharing restrictions, and read, create, or modify files, in certain circumstances involving user accounts that lack home directories.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'samba' Ubuntu package, 2:3.2.3-1ubuntu3, is less than 2:3.2.3-1ubuntu3.6.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-839-1
CVE:	CVE-2009-2813
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230903
Name:	USN-839-1: Samba vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	4.0 - (AV:N/AC:L/Au:S/C:N/I:N/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)

Family:	ubuntu
Description:	smbd in Samba 3.0 before 3.0.37, 3.2 before 3.2.15, 3.3 before 3.3.8, and 3.4 before 3.4.2 allows remote authenticated users to cause a denial of service (infinite loop) via an unanticipated oplock break notification reply packet.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'samba' Ubuntu package, 2:3.2.3-1ubuntu3, is less than 2:3.2.3-1ubuntu3.6.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-839-1
CVE:	CVE-2009-2906
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230904
Name:	USN-839-1: Samba vulnerabilities
Port:	22/tcp - ssh
Risk factor:	Low risk
CVSS Score:	1.9 - (AV:L/AC:M/Au:N/C:P/I:N/A:N) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	mount.cifs in Samba 3.0 before 3.0.37, 3.2 before 3.2.15, 3.3 before 3.3.8 and 3.4 before 3.4.2, when mount.cifs is installed suid root, does not properly enforce permissions, which allows local users to read part of the credentials file and obtain the password by specifying the path to the credentials file and using the --verbose or -v option.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'samba' Ubuntu package, 2:3.2.3-1ubuntu3, is less than 2:3.2.3-1ubuntu3.6.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-839-1
CVE:	CVE-2009-2948
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Script ID:	230909
Name:	USN-842-1: Wget vulnerability
Port:	22/tcp - ssh
Risk factor:	Medium risk
CVSS Score:	6.8 - (AV:N/AC:M/Au:N/C:P/I:P/A:P) (cdp:ND/td:ND/cr:ND/ir:ND/ar:ND)
Family:	ubuntu
Description:	GNU Wget before 1.12 does not properly handle a '\0' character in a domain name in the Common Name field of an X.509 certificate, which allows man-in-the-middle remote attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to

	SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
Information:	This vulnerability was identified because (1) the version of Ubuntu, 8.10, is less than or equal to 8.10.*; and (2) the version of the 'wget' Ubuntu package, 1.11.4-1ubuntu1, is less than 1.11.4-1ubuntu1.1.
Solution:	Upgrade to the latest version of Ubuntu
Reference:	solution - http://www.ubuntu.com/usn/USN-842-1
CVE:	CVE-2009-3490
History:	First Seen : 2009-11-06 14:45 - New Finding
Target:	intra.example.com - 192.168.200.45 - 2009-11-17 10:57

Scan tracking list

intra.example.com 192.168.200.45