Network Vulnerability Assessment Report

Sorted by host names

Session name: IDC_NC Advance

Start time: 30.08.2005 11:53:50
Finish time: 30.08.2005 11:59:23
Elapsed: 0 day(s) 00:05:33

Total records generated: 21
high severity: 21
Medium severity: 0
informational: 0

203.146.151.10

Service	Severity	Description
http (80/tcp)	High	The remote host is running phpMyAdmin, an open-source software written in PHP to handle the administration of MySQL over the Web. The remote version of this software is vulnerable to arbitrary command execution due to a lack of user-supplied data sanitization. Solution : Upgrade to version 2.6.0-pl2 or newer Risk factor : High BID : 11391
http (80/tcp)	High	The remote host is running a version of PHP earlier than 4.1.2. There are several flaws in how PHP handles multipart/form-data POST requests, any one of which can allow an attacker to gain remote access to the system. Solution : Upgrade to PHP 4.1.2 Risk factor : High CVE : CVE-2002-0081 BID : 4183
http (80/tcp)	High	The remote host is running a version of PHP which is older than 5.0.2 or 4.39. The remote version of this software is vulnerable to a memory disclosure vulnerability in PHP_Variables. An attacker may exploit this flaw to remotely read portions of the memory of the httpd process on the remote host. See also : http://www.php.net/ChangeLog-5.php#5.0.2 Solution : Upgrade to PHP 5.0.2 or 4.3.9 Risk factor : High BID : 11334
ftp (21/tcp)	High	The remote host is running wu-ftpd 2.6.2 or older. There is a bug in this version which may allow an attacker to bypass the

		'restricted-gid' feature and gain unauthorized access to otherwise restricted directories. *** Nessus solely relied on the banner of the remote FTP server, so this might *** be a false positive. Solution : There is no official fix at this time. See the RedHat advisories for more information. Risk factor : High CVE : CVE-2004-0148 BID : 9832 Other references : RHSA:RHSA-2003:307-01
ftp (21/tcp)	High	The remote Wu-FTPd server seems to be vulnerable to a remote overflow. This version contains a remote overflow if s/key support is enabled. The skey_challenge function fails to perform bounds checking on the name variable resulting in a buffer overflow. With a specially crafted request, an attacker can execute arbitrary code resulting in a loss of integrity and/or availability. It appears that this vulnerability may be exploited prior to authentication. It is reported that S/Key support is not enabled by default, though some operating system distributions which ship Wu-Ftpd may have it enabled. *** Nessus solely relied on the banner of the remote server *** to issue this warning, so it may be a false positive. Solution : Upgrade to Wu-FTPd 2.6.3 when available or disable SKEY or apply the patches available at http://www.wu-ftpd.org Risk factor : High CVE : CVE-2004-0185 BID : 8893 Other references : OSVDB:2715, RHSA:RHSA-2004:096-09, DSA:DSA-457-1
ftp (21/tcp)	High	The remote Wu-FTPd server seems to be vulnerable to a remote flaw. This version fails to properly check bounds on a pathname when Wu-Ftpd is compiled with MAIL_ADMIN enabled resulting in a buffer overflow. With a specially crafted request, an attacker can possibly execute arbitrary code as the user Wu-Ftpd runs as (usually root) resulting in a loss of integrity, and/or availability. It should be noted that this vulnerability is not present within the default installation of Wu-Ftpd. The server must be configured using the 'MAIL_ADMIN' option to notify an administrator when a file has been uploaded.

http (80/tcp)	High	The remote host is running a version of PHP which is older than 5.0.3 or 4.3.10. The remote version of this software is vulnerable to various security issues which may, under certain circumstances, to execute arbitrary code on the remote host, provided that we can pass arbitrary data to some functions, or to bypass safe_mode. See also : http://www.php.net/ChangeLog-5.php#5.0.3 Solution : Upgrade to PHP 5.0.3 or 4.3.10 Risk factor : High BID : 11964, 11981, 11992, 12045
http (80/tcp)	High	According to its banner, the version of PHP installed on the remote host is vulnerable to a denial of service attack due to its failure to properly validate file data in the routines 'php_handle_iff' and 'php_handle_jpeg', which are called by the PHP function 'getimagesize'. Using a specially crafted image file, an attacker can trigger an infinite loop when 'getimagesize' is called, perhaps even remotely in the case image uploads are allowed. Solution : Upgrade to PHP 4.3.11 / PHP 5.0.4 or later. Risk factor : Medium CVE : CAN-2005-0524, CAN-2005-0525 BID : 12962, 12963
http (80/tcp)	High	The remote host appears to be running a version of Apache which is older than 1.3.29 There are several flaws in this version, which may allow an attacker to possibly execute arbitrary code through mod_alias and mod_rewrite. You should upgrade to 1.3.29 or newer. *** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive Solution : Upgrade to version 1.3.29 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0542 BID : 8911
ftp (21/tcp)	High	The remote Wu-FTPd server seems to be vulnerable to an off-by-one overflow when dealing with huge directory structures. An attacker may exploit this flaw to obtain a shell on this host. *** Nessus solely relied on the banner of the remote server *** to issue this warning, so it may be a false positive. *** Since Wu-FTPd 2.6.3 has not been released yet and only *** patches are available to fix this issue, this might be *** a false positive. Solution : Upgrade to Wu-FTPd 2.6.3 when available or apply the patches available at http://www.wu-ftpd.org Risk factor : High CVE : CAN-2003-0466

ftp (21/tcp)	High	You seem to be running an FTP server which is vulnerable to the 'glob heap corruption' flaw. An attacker may use this problem to execute arbitrary commands on this host. *** Nessus relied solely on the banner of the server to issue this warning, *** so this alert might be a false positive *** NOTE: must have a valid username/password to fully check this vulnerability Solution : Upgrade your ftp server software to the latest version. Risk factor : High CVE : CAN-2001-0249, CVE-2001-0550 BID : 2550, 3581

203.146.151.9

Service	Severity	Description
http (80/tcp)	High	The remote host appears to be running a version of Apache which is older than 1.3.29 There are several flaws in this version, which may allow an attacker to possibly execute arbitrary code through mod_alias and mod_rewrite. You should upgrade to 1.3.29 or newer. *** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive Solution : Upgrade to version 1.3.29 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0542 BID : 8911
ftp (21/tcp)	High	The remote Wu-FTPd server seems to be vulnerable to a remote flaw. This version fails to properly check bounds on a pathname when Wu-Ftpd is compiled with MAIL_ADMIN enabled resulting in a buffer overflow. With a specially crafted request, an attacker can possibly execute arbitrary code as the user Wu-Ftpd runs as (usually root) resulting in a loss of integrity, and/or availability. It should be noted that this vulnerability is not present within the default installation of Wu-Ftpd. The server must be configured using the 'MAIL_ADMIN' option to notify an administrator when a file has been uploaded. *** Nessus solely relied on the banner of the remote server

ftp (21/tcp)	High	The remote Wu-FTPd server seems to be vulnerable to a remote overflow. This version contains a remote overflow if s/key support is enabled. The skey_challenge function fails to perform bounds checking on the name variable resulting in a buffer overflow. With a specially crafted request, an attacker can execute arbitrary code resulting in a loss of integrity and/or availability. It appears that this vulnerability may be exploited prior to authentication. It is reported that S/Key support is not enabled by default, though some operating system distributions which ship Wu-Ftpd may have it enabled. *** Nessus solely relied on the banner of the remote server *** to issue this warning, so it may be a false positive. Solution : Upgrade to Wu-FTPd 2.6.3 when available or disable SKEY or apply the patches available at http://www.wu-ftpd.org Risk factor : High CVE : CVE-2004-0185 BID : 8893 Other references : OSVDB:2715, RHSA:RHSA-2004:096-09, DSA:DSA-457-1
ftp (21/tcp)	High	The remote Wu-FTPd server seems to be vulnerable to an off-by-one overflow when dealing with huge directory structures. An attacker may exploit this flaw to obtain a shell on this host. *** Nessus solely relied on the banner of the remote server *** to issue this warning, so it may be a false positive. *** Since Wu-FTPd 2.6.3 has not been released yet and only *** patches are available to fix this issue, this might be *** a false positive. Solution : Upgrade to Wu-FTPd 2.6.3 when available or apply the patches available at http://www.wu-ftpd.org Risk factor : High CVE : CAN-2003-0466 BID : 8315 Other references : RHSA:RHSA-2003:245-01, SuSE:SUSE-SA:2003:032
http (80/tcp)	High	According to its banner, the version of PHP installed on the remote host is vulnerable to a denial of service attack due to its failure to properly validate file data in the routines 'php_handle_iff' and 'php_handle_jpeg', which are called by the PHP function 'getimagesize'. Using a specially crafted image file, an attacker can trigger an infinite loop when 'getimagesize' is called, perhaps even remotely in the case image uploads are allowed. Solution : Upgrade to PHP 4.3.11 / PHP 5.0.4 or later. Risk factor : Medium CVE : CAN-2005-0524, CAN-2005-0525 BID : 12962, 12963
http (80/tcp)	High	The remote host is running a version of PHP which is older than 5.0.3

		or 4.3.10. The remote version of this software is vulnerable to various security issues which may, under certain circumstances, to execute arbitrary code on the remote host, provided that we can pass arbitrary data to some functions, or to bypass safe_mode. See also : http://www.php.net/ChangeLog-5.php#5.0.3 Solution : Upgrade to PHP 5.0.3 or 4.3.10 Risk factor : High BID : 11964, 11981, 11992, 12045
http (80/tcp)	High	The remote host is running a version of PHP earlier than 4.1.2. There are several flaws in how PHP handles multipart/form-data POST requests, any one of which can allow an attacker to gain remote access to the system. Solution : Upgrade to PHP 4.1.2 Risk factor : High CVE : CVE-2002-0081 BID : 4183
ftp (21/tcp)	High	You seem to be running an FTP server which is vulnerable to the 'glob heap corruption' flaw. An attacker may use this problem to execute arbitrary commands on this host. *** Nessus relied solely on the banner of the server to issue this warning, *** so this alert might be a false positive *** NOTE: must have a valid username/password to fully check this vulnerability Solution : Upgrade your ftp server software to the latest version. Risk factor : High CVE : CAN-2001-0249, CVE-2001-0550 BID : 2550, 3581
ftp (21/tcp)	High	The remote host is running wu-ftpd 2.6.2 or older. There is a bug in this version which may allow an attacker to bypass the 'restricted-gid' feature and gain unauthorized access to otherwise restricted directories. *** Nessus solely relied on the banner of the remote FTP server, so this might *** be a false positive. Solution : There is no official fix at this time. See the RedHat advisories for more information. Risk factor : High CVE : CVE-2004-0148 BID : 9832 Other references : RHSA:RHSA-2003:307-01
http (80/tcp)	High	The remote host is running a version of PHP which is older than 5.0.2

		or 4.39. The remote version of this software is vulnerable to a memory disclosure vulnerability in PHP_Variables. An attacker may exploit this flaw to remotely read portions of the memory of the httpd process on the remote host. See also : http://www.php.net/ChangeLog-5.php#5.0.2 Solution : Upgrade to PHP 5.0.2 or 4.3.9 Risk factor : High BID : 11334