Vulnerability Status

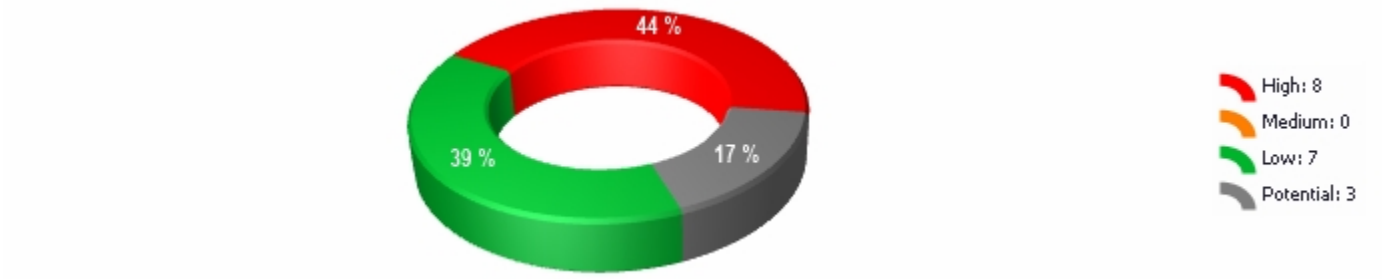
Description	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.
Generated on	29-10-2015 12:28:14
Generated by	Mario

Advanced Settings

Report items	All
Target	MARIO
Grouped by	'Computer' - Ascending AND 'Vulnerability Severity' - Descending
Sorted by	'Vulnerability Timestamp' - Ascending

Reviewed by _____ Reviewed Date _____ Signature _____

Vulnerability Distribution by Severity

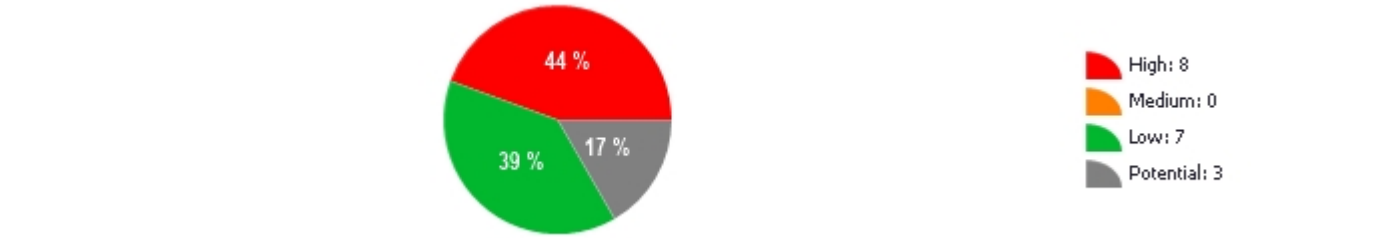


Vulnerability Distribution by Computer

Computer/IP	High	Medium	Low	Potential
MARIO	8	0	7	3

Vulnerability Listing by Computer

MARIO



High

Vulnerability Name	Product	Severity	CVSS Score	Timestamp
AutoRun is enabled	N/A	High	-	2007-05-10
Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a security risk in the case where a CD or removable disk containing malware that automatically installs itself once the disc is inserted.It is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives.				
MS11-025: Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538243)	Developer Tools, Runtimes, and Redistributables	High	-	2012-01-24
OVAL:22538: A router or firewall allows source routed packets from arbitrary hosts (CVE-1999-0510)	N/A	High	7,5	2014-03-13
A router or firewall allows source routed packets from arbitrary hosts.				
MS14-059: Security Update for Microsoft ASP.NET MVC 4.0 (KB2993928)	ASP.NET Web and Data Frameworks	High	-	2014-10-14
VLC221: VLC Media Player 2.2.1 exe	VLC Media Player	High	-	2015-04-17
Microsoft Silverlight (KB3080333)	Silverlight	High	-	2015-08-11
HT205221: iTunes 12.3 for Windows (64-bit)	iTunes	High	-	2015-09-16
JAVA8065: Java Runtime Environment 8.0 x64 Update 65	Java Runtime Environment	High	-	2015-10-21

Vulnerability Listing by Computer

Low

Vulnerability Name	Product	Severity	CVSS Score	Timestamp
Shutdown without logon	N/A	Low	-	2002-01-01
Anybody is allowed to shutdown this computer. For more information, visit: http://support.microsoft.com/kb/313924				
AutoShareServer	Windows	Low	-	2002-01-01
The administrative shares (C$,D$,ADMIN$,etc) are available on this machine. For Internal networks these are normally turned on for administrative purposes. For Web server(s) these are normally turned off in order to solidify the possible entry points (since it is more exposed to attacks.). If you don't use them set HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer to 0 to prevent creation of these shares. For more information, visit: http://support.microsoft.com/kb/245117				
AutoShareWKS	Windows	Low	-	2002-01-01
The administrative shares (C$,D$,ADMIN$,etc) are available on this machine. For Internal networks these are normally turned on for administrative purposes. For Web server(s) these are normally turned off in order to solidify the possible entry points (since it is more exposed to attacks.). If you don't use them set HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks to 0 to prevent creation of these shares. For more information, visit: http://support.microsoft.com/kb/245117				
Cached Logon Credentials	Windows NT	Low	-	2002-01-01
Microsoft Windows NT caches the logon information of users who would have logged on, so that they would be able to logon when the server is unavailable. When a domain controller is unavailable and a user's logon information is cached, the user will still be allowed to logon. The cache can hold up from 0 to 50 logon attempts, with the value of 0 disabling logon caching. If the value is set to a high value and an administrator logs in to computers to solve specific problems, an attacker might obtain the credentials of the administrator at a later stage, and logon with such an account, having powerful privileges. The registry value for setting this type of caching is: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount. Ideally it should be set to either 0 to disable caching, or else it should be set to 1 to provide for functionality (allowing the last user to logon immediately next time) and security.				
Service running: HTTP	N/A	Low	-	2007-01-31
If this is not an web server, the HTTP service is most likely unnecessary.				
Service running: MySQL	N/A	Low	-	2007-01-31
If this is not a database server, the MySQL service is most likely unnecessary.				
IM installed: Skype	Skype	Low	-	2008-01-17
Skype instant messaging client is installed.				

Potential

Vulnerability Name	Product	Severity	CVSS Score	Timestamp
PHP module running (web server)	PHP	Potential	-	2002-01-01
PHP is installed on this web server.				
USB devices installed over time	N/A	Potential	-	2008-11-17
This check generates a list of all USB devices that have been connected to the scanned computer. - SONY CD-ROM USB Device - Kingston DataTraveler 2.0 USB Device - Kingston DT 101 II USB Device - Philips USB Flash Drive USB Device - SanDisk Cruzer Pop USB Device - Seagate FreeAgent GoFlex USB Device				
User Mario never logged on	N/A	Potential	-	N/A

Vulnerability Listing by Computer

It is recommended to remove this account if not used