



 **GLASSHOUSE**

SAFEGUARD WEB-BASED PORTAL

DASHBOARD EXAMPLES

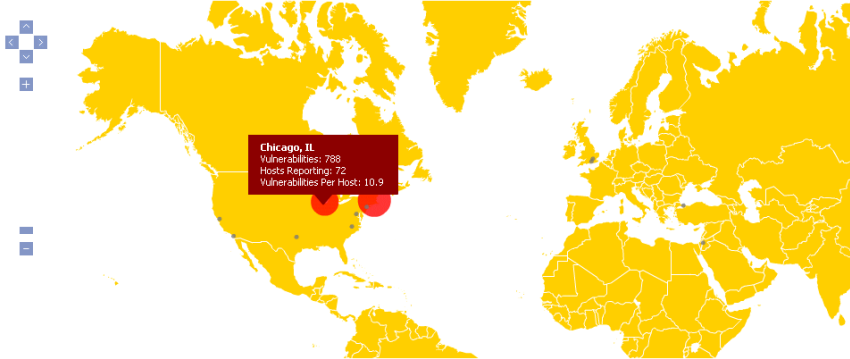
March 2009

MAIN DASHBOARD

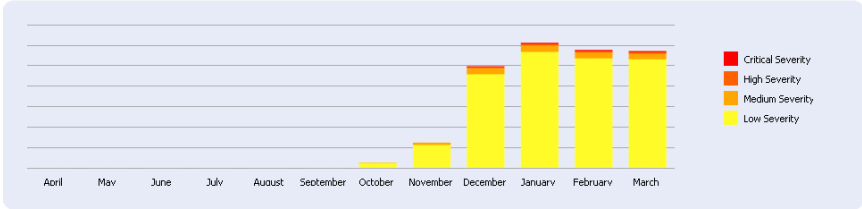
Vulnerability Management Dashboard

Vulnerabilities by Location

Comparing locations by average number of vulnerabilities per host, [compare by number of vulnerabilities](#)



Trend Overview



Trend Analysis

Monthly Change:
1143 issues (-32)
Note: only issues with a low severity or above are included

New Systems	0 systems
Existing Systems	87 systems / 1143 issues
Closed Issues	32 issues

Key Statistics

92% Percent of Hosts with Vulnerabilities
12.28 Vulnerabilities per System (Average)

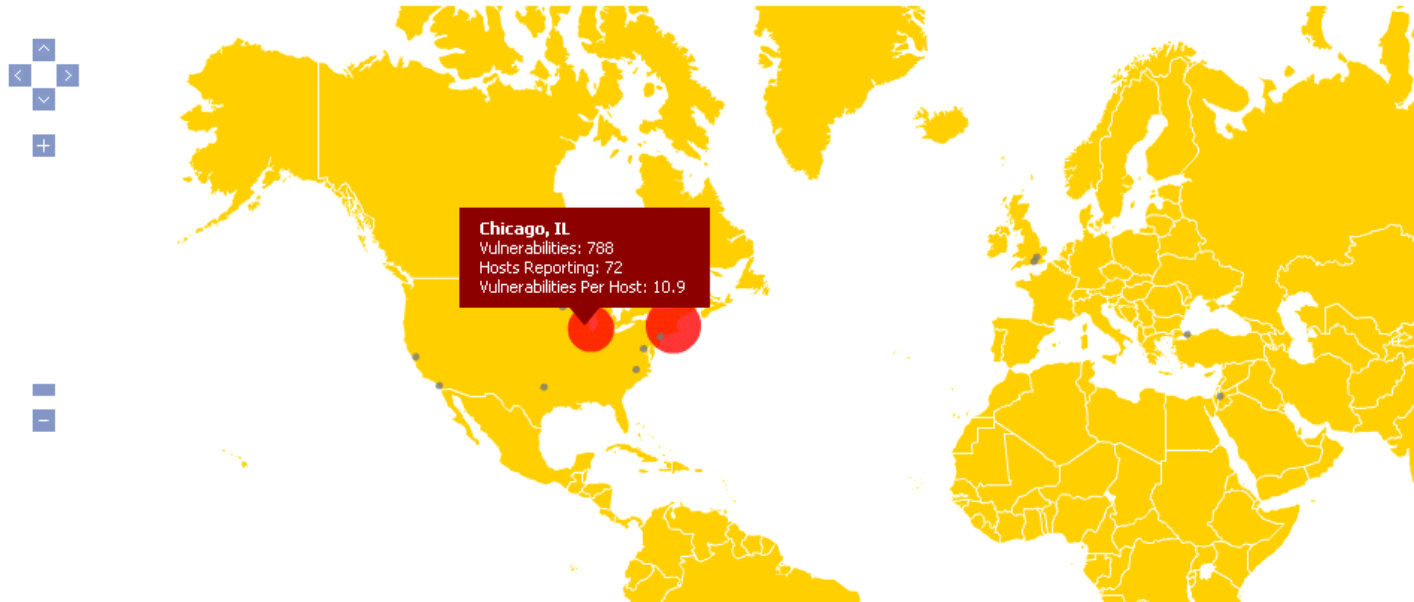
Critical Severity Vulnerability:	7 Systems (7%)
High Severity Vulnerability:	12 Systems (12%)
Medium Severity Vulnerability:	21 Systems (22%)
Low Severity Vulnerability:	87 Systems (92%)

A high-level view of vulnerabilities including:

- Geographical distribution - *which sites are the most vulnerable*
- Vulnerability trend - *is the problem getting worse*
- Trend analysis



GEOGRAPHICAL VIEW



Geographical view

Provides statistics about each site such as:

- Number of vulnerabilities
- Number of systems scanned
- Average number of vulnerabilities per host

Each location can be clicked on to drill into more detail.



Trend Analysis

Provides information about the trend by indicating:

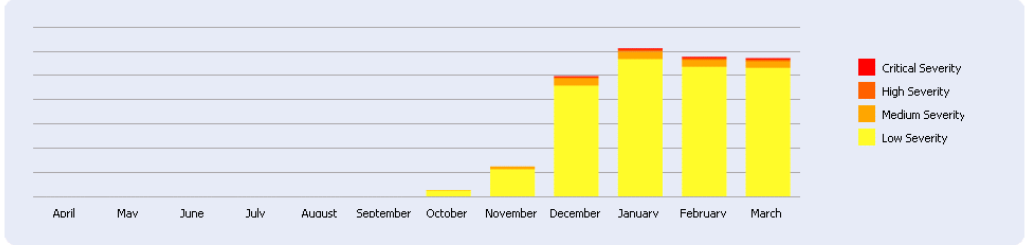
- Whether the trend is up or down and by how much
- If the increase in issues due to newly discovered systems (i.e. the trend is up because the customer is scanning more systems)
- If the Increase/decrease is due to vulnerabilities on existing systems
- The number of issues that have been closed

Key Statistics


Provides information that indicates the severity of the situation

- The number of hosts with vulnerabilities (broken down by severity)
- The average number of vulnerabilities per system

Trend Overview



Trend Analysis

Monthly Change:
 1143 issues **(-32)**
 Note: only issues with a low severity or above are included

New Systems	0 systems
Existing Systems	87 systems / 1143 issues
Closed Issues	32 issues

Key Statistics

92% Percent of Hosts with Vulnerabilities

12.28 Vulnerabilities per System (Average)

Critical Severity Vulnerability:	7 Systems (7%)
High Severity Vulnerability:	12 Systems (12%)
Medium Severity Vulnerability:	21 Systems (22%)
Low Severity Vulnerability:	87 Systems (92%)

VULNERABLE SYSTEMS VIEW

Observations by Host

Host name:
To filter the findings, include the part of a DNS name, NetBIOS machine name, IP address or MAC Address

Operating system:

Event name:
Enter an event to filter the list to hosts that have the associated observation

Severity:

Add category filter:

Hosts				
<input type="checkbox"/> Server-2251 (-4)	40	5	1	1
<input type="checkbox"/> LAPTOP-7 (-5)	26	6	1	1
<input type="checkbox"/> Server-13762(-3)	27	3	2	
<input type="checkbox"/> Server-891076	21	3	5	
<input type="checkbox"/> LAPTOP-267905 (-9)	25	3	1	
<input type="checkbox"/> LAPTOP-511064	24	1	1	
<input type="checkbox"/> LAPTOP-725871	21	1		
<input type="checkbox"/> 57676Host	19	2		
<input type="checkbox"/> TEST-437363	16	2	2	1














A list of vulnerable systems sorted with the most vulnerable hosts first.

Note that the list can be filtered by:

- Asset category – eg. *show me all Email Servers in New York*
- Operating system
- Severity of the issues on the host – eg. *which systems have a critical issue*
- System name
- Hosts with a specific issue – eg. *which hosts have SMB Null Sessions*
- Any combination of the above

VULNERABLE OPERATING SYSTEMS VIEW

Number of Vulnerable Hosts per Operating System

 Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3	27	1	2	1
 Microsoft Windows XP Professional	7	1	1	
 Microsoft Windows Server 2003	5		3	
 Microsoft Windows 2000, Microsoft Windows XP	3	1		
 Microsoft Windows Server 2003 Service Pack 2	2	2		
 Microsoft XP Professional Service Pack 2	3	1		
 Alcatel VoIP terminal	1	1		
 Microsoft Windows 2000, Microsoft Windows Server 2003	1	1		
 Mac OS X 10.5.5 (intel)	1			
 Linux Kernel 2.2	1			
 FreeBSD 6.0, FreeBSD 6.1, FreeBSD 6.2, FreeBSD 6.3	1			
 Linux Kernel 2.6	1			
 HP ProCurve Switch	1			

A list of vulnerable operating systems

The number of vulnerable hosts with a given OS can be filtered by:

- Asset category – eg. *what is the most common OS with a vulnerability in New York*
- Name
- A combination of the above

VULNERABILITY DESCRIPTION VIEW

GLASSHOUSE

Reporting Assets Tickets Profile

Hello Luke Murphey [\[Logout\]](#)

Dashboard » Observations by Event » Observations on Server-209234 » SMB NULL session

SMB NULL session

Risk Factor

Undefined

Description

The remote host is running Microsoft Windows, and it was possible to log into it using a NULL session (ie, with no login or password). An unauthenticated remote attacker can leverage this issue to get information about the remote host.

Solution

Null sessions can be disabled using on of the following methods:

Windows XP

Open the local security policy (secpol.msc) and enable the following: security options:

Network Access: Do not allow anonymous enumeration of SAM accounts
Network access: Do not allow anonymous enumeration of SAM accounts and shares

Windows 2000

Open the local security policy (secpol.msc) and enable the following:

Additional restrictions for anonymous connections

Open the local security policy (secpol.msc) and enable the following:

Windows NT 4.0 SP3 and later

Open the registry editor (regedit.exe) and locate "restrictanonymou" in the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

Set the value "restrictanonymou" to 1 to disable null sessions.

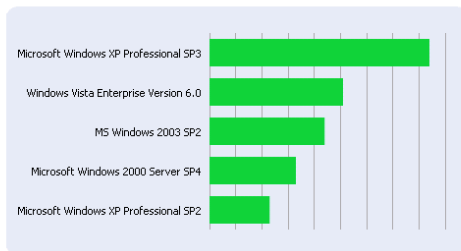
Overview

Issue Family	Windows
Issue ID	26920
Issue Type	Infos
First Observed	1:34 a.m. Sep 02, 2008
Last Observed	12:32 a.m. Jan 06, 2009
Create Ticket	[Create Ticket From This Event]
CVE	CVE-2002-1117
BID	494

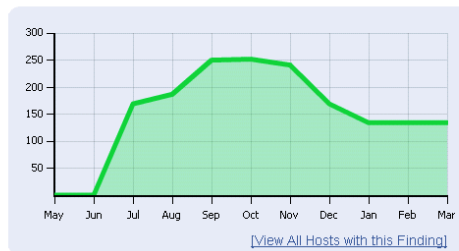
Provides details about the vulnerability including:

- A description of the problem
- Solutions to fix the problems (links to vendor patches, etc.)
- Trend summary – eg. *is this issue becoming more common*
- Top Operating Systems with the issue

Top Operating Systems With This Observation



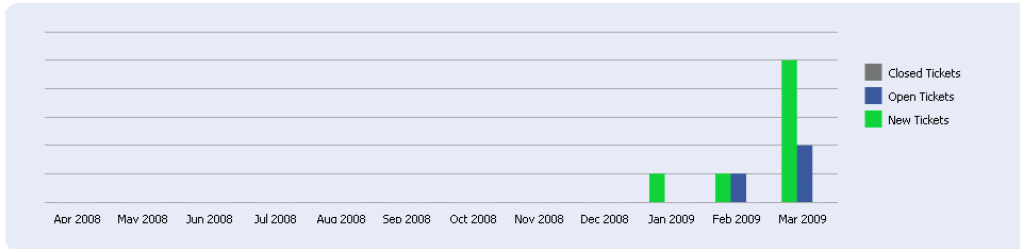
Observation History (Entire Organization)



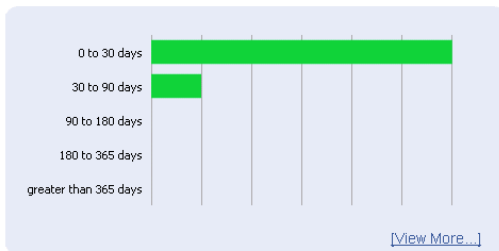


TICKET VIEW

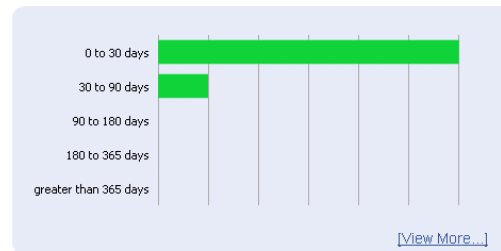
Status Overview (Entire Organization)



Open Ticket Age (Entire Organization)



Open Ticket Age (Your Tickets)



Ticket Remediation Quality (Entire Organization)

Ticket Response Performance:
100.00% closed within deadline

Average Closure Time	No tickets closed recently
Tickets Closed	0 Tickets
Overdue Tickets Open	2 Tickets (14.29%)
Total Tickets Open	14 Tickets

Ticket Remediation Quality (Your Tickets)

Ticket Response Performance:
100.00% closed within deadline

Average Closure Time	No tickets closed recently
Tickets Closed	0 Tickets
Overdue Tickets Open	2 Tickets (14.29%)
Total Tickets Open	14 Tickets

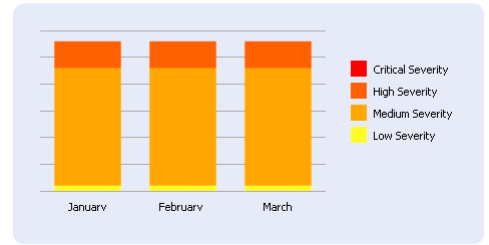
Ticket details

- Service level metrics (based on the policy defined by the customer)
- Number of ticket that are new, closed or open
- The number of tickets open by age
- Ticket closure metrics (percentage closed according to policy)

HOST VIEW

Host Overview

Observation History



Host Information

DNS Name	Server912.Customer1.com
Machine Name	Server-209234
IP Address	10.51.103.68
Operating System	Windows Server 2008
Priority	Undefined [Edit Asset Record]
Ticketing	[Create Ticket] [View Tickets]
Total Issues	28 [Export Issues to CSV]

This system is within the following categories: [\[click to view/hide\]](#)

Name	Type	Priority
Servers	System Function	Undefined
eCommerce	System Function	High
Paris, France	Location	Undefined

Observations

First Observed	Last Observed	Name	Severity
Aug 12, 2008	2 months ago	SMB log in	High
Jul 01, 2008	2 months ago	SMB registry can not be accessed by the scanner	High
Jul 01, 2008	2 months ago	Weak Supported SSL Ciphers Suites	High
Sep 02, 2008	2 months ago	SMB NULL session	High
Sep 02, 2008	2 months ago	SMB LanMan Pipe Server browse listing	High

Provides list of issues a given host.
Includes information such as:

- Trending of issues on the host
- Information about the host (IP address, DNS name, machine name, etc.)
- Asset categories that the host is part of
- List of issues on the host