Vulnerability Status Summary

Rsam Vulnerability Management Reports

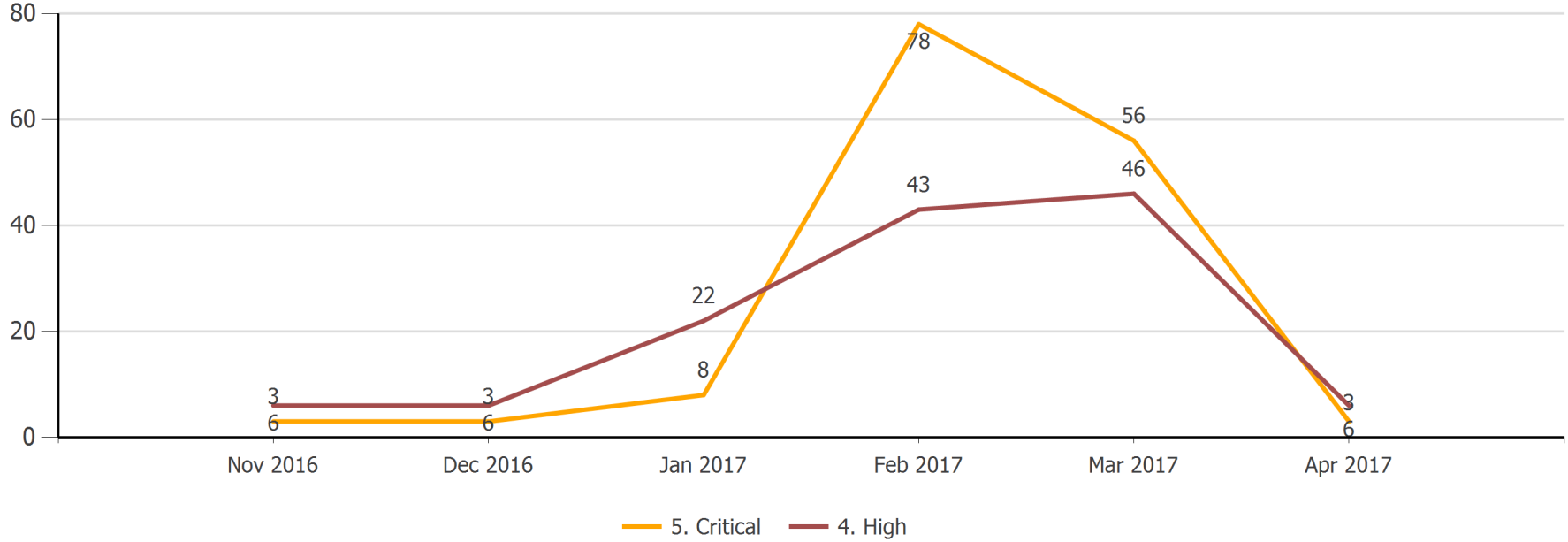
Report Date: 01-16-2018

Overview

The following report summarizes open, critical and high risk vulnerabilities for IT Host assets as of the report generation date. For the purposes of this report, "Open" vulnerabilities are those which have not been remediated or confirmed as a false positive, do not have approved compensating controls, or the risk has not been accepted.

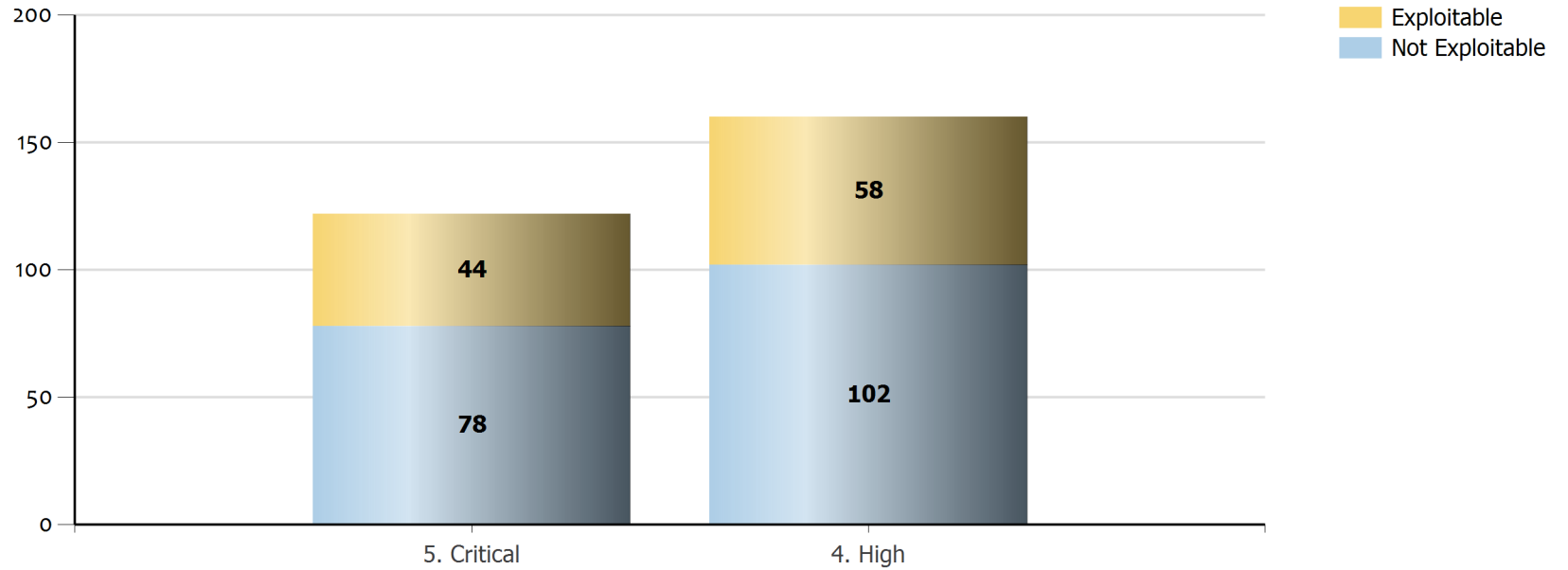
Trend of Average Days Open by Severity

Understanding the time it takes to remediate vulnerabilities is valuable in assessing how effective a company's remediation process is. This information can assist in identifying areas for process improvement and can support the need for additional resources. The following chart displays the average number of days it takes for a vulnerability to move from "Open" to "Closed".



Vulnerabilities by Severity and Exploitability

While each vulnerability has an assigned risk rating, additional factors, such as known exploits, can be used to escalate the risk rating or adjust the prioritization of remediation efforts. The chart shows the breakdown across all open, critical and high vulnerabilities.



*Exploitability is based on an Exploit Source being reported by the scanner

Exploitable Vulnerability Details

This table lists additional information for each of the exploitable vulnerabilities represented in the chart above.

Vendor Vulnerability ID	Vulnerability Name	# of Instances	Scanner	Risk Rating
19197	Oracle January Security Update Multiple Vulnerabilities (January 2006)	5	Qualys VM	5. Critical
19548	Oracle April 2010 Security Update Multiple Vulnerabilities	2	Qualys VM	5. Critical
19589	Oracle Database October 2010 Security Update Multiple Vulnerabilities	2	Qualys VM	5. Critical
77823	Bash Remote Code Execution (Shellshock)	2	Tenable Security Center	5. Critical
78067	Bash Remote Code Execution (CVE-2014-6277 / CVE-2014-6278) (Shellshock)	2	Tenable Security Center	5. Critical
19203	Oracle Critical Patch Update - April 2006	1	Qualys VM	5. Critical
55862	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	1	Tenable Security Center	5. Critical
56569	CentOS 5 : kernel (CESA-2011:1386)	1	Tenable Security Center	5. Critical
57405	CentOS 4 / 5 : krb5 (CESA-2011:1851)	1	Tenable Security Center	5. Critical
57777	CentOS 4 / 5 / 6 : firefox (CESA-2012:0079)	1	Tenable Security Center	5. Critical
58663	CentOS 5 / 6 : samba (CESA-2012:0465)	1	Tenable Security Center	5. Critical
59481	CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)	1	Tenable Security Center	5. Critical
62593	Oracle Java SE Multiple Vulnerabilities (October 2012 CPU)	1	Tenable Security Center	5. Critical
62630	CentOS 5 : java-1.6.0-openjdk (CESA-2012:1385)	1	Tenable Security Center	5. Critical
64454	Oracle Java SE Multiple Vulnerabilities (February 2013 CPU)	1	Tenable Security Center	5. Critical
64512	CentOS 5 : java-1.6.0-openjdk (CESA-2013:0246)	1	Tenable Security Center	5. Critical

Vendor Vulnerability ID	Vulnerability Name	# of Instances	Scanner	Risk Rating
65064	CentOS 5 : java-1.6.0-openjdk (CESA-2013:0604)	1	Tenable Security Center	5. Critical
65995	Oracle Java SE Multiple Vulnerabilities (April 2013 CPU)	1	Tenable Security Center	5. Critical
66205	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	1	Tenable Security Center	5. Critical
66932	Oracle Java SE Multiple Vulnerabilities (June 2013 CPU)	1	Tenable Security Center	5. Critical
67183	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	1	Tenable Security Center	5. Critical
70472	Oracle Java SE Multiple Vulnerabilities (October 2013 CPU)	1	Tenable Security Center	5. Critical
73985	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	1	Tenable Security Center	5. Critical
76557	SuSE 11.3 Security Update : Linux kernel (SAT Patch Numbers 9488 / 9491 / 9493)	1	Tenable Security Center	5. Critical
77835	CentOS 5 / 6 / 7 : bash (CESA-2014:1293) (Shellshock)	1	Tenable Security Center	5. Critical
77850	SuSE 11.3 Security Update : bash (SAT Patch Number 9740)	1	Tenable Security Center	5. Critical
77879	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	1	Tenable Security Center	5. Critical
77958	SuSE 11.3 Security Update : bash (SAT Patch Number 9780)	1	Tenable Security Center	5. Critical
79127	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)	1	Tenable Security Center	5. Critical
80491	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (3020393)	1	Tenable Security Center	5. Critical
81470	RHEL 6 : samba (RHSA-2015:0251)	1	Tenable Security Center	5. Critical
81471	RHEL 7 : samba (RHSA-2015:0252)	1	Tenable Security Center	5. Critical
81508	SuSE 11.3 Security Update : Samba (SAT Patch Number 10321)	1	Tenable Security Center	5. Critical

Vendor Vulnerability ID	Vulnerability Name	# of Instances	Scanner	Risk Rating
95001	X-Window Sniffing	1	Qualys VM	5. Critical
78385	Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)	3	Nessus	4. High
12260	Apache HTTP Server Multiple Cross-Site Scripting Vulnerabilities	2	Qualys VM	4. High
19260	Oracle October 2008 Security Update Multiple Vulnerabilities	2	Qualys VM	4. High
19267	Oracle January 2009 Security Update Multiple Vulnerabilities	2	Qualys VM	4. High
19463	Oracle April 2009 Security Update Multiple Vulnerabilities	2	Qualys VM	4. High
19498	Oracle October 2009 Security Update Multiple Vulnerabilities	2	Qualys VM	4. High
19608	Oracle Database January 2011 Security Update Multiple Vulnerabilities (CPUJAN2011)	2	Qualys VM	4. High
19616	Oracle Database April 2011 Security Update Multiple Vulnerabilities (CPUAPR2011)	2	Qualys VM	4. High
53382	MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)	1	Tenable Security Center	4. High
61681	Oracle Java SE 7 < Update 7 Multiple Vulnerabilities	1	Tenable Security Center	4. High
63521	Oracle Java SE 7 < Update 11 Multiple Vulnerabilities	1	Tenable Security Center	4. High
65052	Oracle Java JDK / JRE 7 < Update 17 Remote Code Execution (Windows)	1	Tenable Security Center	4. High
72930	MS14-012: Cumulative Security Update for Internet Explorer (2925418)	1	Tenable Security Center	4. High
72934	MS14-015: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2930275)	1	Tenable Security Center	4. High
73415	MS14-018: Cumulative Security Update for Internet Explorer (2950467)	1	Tenable Security Center	4. High
73751	SuSE 11.3 Security Update : Python (SAT Patch Number 9075)	1	Tenable Security Center	4. High
73805	MS14-021: Security Update for Internet Explorer (2965111)	1	Tenable Security Center	4. High
73986	MS14-027: Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege (2962488)	1	Tenable Security Center	4. High

Vendor Vulnerability ID	Vulnerability Name	# of Instances	Scanner	Risk Rating
73988	MS14-029: Security Update for Internet Explorer (2962482)	1	Tenable Security Center	4. High
74033	SuSE 11.3 Security Update : Linux Kernel (SAT Patch Numbers 9233 / 9236 / 9237)	1	Tenable Security Center	4. High
74427	MS14-035: Cumulative Security Update for Internet Explorer (2969262)	1	Tenable Security Center	4. High
74462	SuSE 11.3 Security Update : Linux Kernel (SAT Patch Numbers 9328 / 9329 / 9330)	1	Tenable Security Center	4. High
76406	MS14-037: Cumulative Security Update for Internet Explorer (2975687)	1	Tenable Security Center	4. High
76409	MS14-040: Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (2975684)	1	Tenable Security Center	4. High
77169	MS14-051: Cumulative Security Update for Internet Explorer (2976627)	1	Tenable Security Center	4. High
77572	MS14-052: Cumulative Security Update for Internet Explorer (2977629)	1	Tenable Security Center	4. High
77895	RHEL 5 / 6 / 7 : bash (RHSA-2014:1306)	1	Nessus	4. High
78431	MS14-056: Cumulative Security Update for Internet Explorer (2987107)	1	Tenable Security Center	4. High
78433	MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)	1	Tenable Security Center	4. High
78438	MS14-062: Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254)	1	Tenable Security Center	4. High
78439	MS14-063: Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege (2998579)	1	Tenable Security Center	4. High
79125	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)	1	Tenable Security Center	4. High
79126	MS14-065: Cumulative Security Update for Internet Explorer (3003057)	1	Tenable Security Center	4. High
79130	MS14-070: Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)	1	Tenable Security Center	4. High
79311	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)	1	Tenable Security Center	4. High

Vendor Vulnerability ID	Vulnerability Name	# of Instances	Scanner	Risk Rating
79828	MS14-080: Cumulative Security Update for Internet Explorer (3008923)	1	Tenable Security Center	4. High
80105	CentOS 5 : kernel (CESA-2014:2008)	1	Tenable Security Center	4. High
80492	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (3021674)	1	Tenable Security Center	4. High
81025	CentOS 5 : glibc (CESA-2015:0090) (GHOST)	1	Tenable Security Center	4. High
81262	MS15-009: Security Update for Internet Explorer (3034682)	1	Tenable Security Center	4. High
81263	MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)	1	Tenable Security Center	4. High
81733	MS15-018: Cumulative Security Update for Internet Explorer (3032359)	1	Tenable Security Center	4. High
81735	MS15-020: Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (3041836)	1	Tenable Security Center	4. High
81736	MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (3032323)	1	Tenable Security Center	4. High
81739	MS15-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)	1	Tenable Security Center	4. High
82428	SuSE 11.3 Security Update : MySQL (SAT Patch Number 10387)	1	Tenable Security Center	4. High
82495	RHEL 5 / 6 / 7 : firefox (RHSA-2015:0766)	1	Tenable Security Center	4. High
82770	MS15-032: Cumulative Security Update for Internet Explorer (3038314)	1	Tenable Security Center	4. High
82772	MS15-035: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)	1	Tenable Security Center	4. High
82774	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)	1	Tenable Security Center	4. High
88148	CentOS 7 : kernel (CESA-2016:0064)	1	Tenable Security Center	4. High

Most Vulnerable Assets

Identifying the most vulnerable assets and the most prevalent vulnerabilities across a business' environment is useful in prioritizing remediation efforts and facilitating root cause analysis.

The following table lists the top 10 assets with the highest number of open, critical and high vulnerabilities. Visibility of certain columns, such as Zone, is dependent upon the existence of such data in Rsam.

NOTE: The chart is limited to 10 rows even in the event that multiple items are tied for last place.

Asset IP Address	Asset Name	Zone	Operating System	# of Vulnerabilites	Critical	High
172.26.16.166	NETBIOS016	Internal	Windows Server 2016	61	16	45
172.26.16.211	NETBIOS017	DMZ	Windows Server 2016	40	32	8
172.26.17.98	NETBIOS020	External	Windows Server 2008	27	14	13
1.1.37.32	NETBIOS032	Internal	Windows Server 2016	23	9	14
1.1.37.35	NETBIOS033	Internal	Windows Server 2016	23	9	14
10.2.57.255	NETBIOS255	DMZ	Windows Server 2008	16	9	7
10.2.63.192	NETBIOS192	DMZ	RedHat Enterprise Linux 7	15	8	7
172.26.16.243	NETBIOS018	Internal	Solaris 11	14	4	10
1.1.37.31	NETBIOS031	External	RedHat Enterprise Linux 7	7	5	2
127.0.0.1	NETBIOS014	Internal	Windows Server 2008	7	2	5

Most Prevalent Open Vulnerabilities

The following table outlines reported vulnerability details for the top 10 open, critical/high vulnerabilities. In addition, the total instances of each vulnerability is divided across the total asset inventory within Rsam to illustrate the pervasiveness across the environment. Supporting details for each vulnerability listed can be found by clicking on the link in the Vendor Vulnerability ID column.

NOTE: The chart is limited to 10 rows even in the event that multiple items are tied for last place.

Vendor Vulnerability ID	Vulnerability Name	Scanner	% of Assets Affected	# of Instances	Risk Rating
19197	Oracle January Security Update Multiple Vulnerabilities (January 2006)	Qualys VM	8.47%	5	5. Critical
19203	Oracle Critical Patch Update - April 2006	Qualys VM	8.47%	5	5. Critical
19210	Oracle Critical Patch Update Missing - July 2006	Qualys VM	8.47%	5	5. Critical
19121	Oracle Listener Input Validation Vulnerabilities	Qualys VM	5.08%	3	5. Critical
116377	iDefense Exclusive: Multiple Vendor CUPS texttops Memory Corruption Vulnerability	Qualys VM	10.17%	6	4. High
12260	Apache HTTP Server Multiple Cross-Site Scripting Vulnerabilities	Qualys VM	10.17%	6	4. High
38469	OpenSSH GSSAPI Credential Disclosure Vulnerability	Qualys VM	10.17%	6	4. High
38546	Nagios Content-Length Integer Overflow Vulnerability	Qualys VM	6.78%	4	4. High
19073	Multiple Oracle Buffer Overflow Vulnerabilities	Qualys VM	5.08%	3	4. High
19076	Oracle Database Link Buffer Overflow Vulnerability	Qualys VM	5.08%	3	4. High

Open Vulnerabilities by Scanner

Understanding how vulnerabilities are reported by individual scanners is integral in ensuring the business' vulnerability detection processes are optimal. For example, this data may prove helpful when reviewing vulnerabilities identified by perimeter vs. internal scans, as well as, comparing completeness and/or accuracy of scan results reliant on successful authentication.

Scanner	# Open Vulnerabilities	Critical	High
Tenable Security Center	155	71	84
Qualys VM	90	33	57
NeXpose	35	18	17
Nessus	2	0	2

Most Vulnerable Ports

Similarly, many vulnerabilities can be present across multiple ports. The summation of these results can assist in detecting potential use of unauthorized ports and/or additional network-layer controls that may be required to mitigate vulnerable ports required by the business.

Port	Protocol	# of Vulnerabilities
445	TCP	61
1636	tcp	23
1716	tcp	23
22	tcp	12
1706	tcp	12
1668	tcp	6
80	tcp	4
8008	tcp	2
6001	tcp	1