Known Issues with Target Devices and Vulnerability Scanning

Abstract

Description of systems that could potentially be adversely affected by scan traffic.

Author

Qualys Support

Distribution: Public Release
Status: Final
Revision: 4
Date: 11 July 2016

Qualys, Inc.
1600 Bridge Parkway, Suite 201
Redwood Shores, CA 94065
Telephone: (650) 801-6100
Web: www.qualys.com

Table of Contents

1 Introduction

Scanning for security vulnerabilities on your network can cause potential impact to select systems and configurations. Qualys would like to bring to your attention a few known issues on certain target systems. For each issue, there is current information and a resolution when available. If you have any of these systems on your network, be sure to check the vendor references provided for the latest information.

For the latest version of this document please visit Qualys Community Help Center at https://community.qualys.com/community/help . Qualys Support makes every effort to keep this document up-to-date, incorporating the latest information from our customers on a regular basis. We encourage our customers to visit the community and contribute to the content of this document.

1.1 Document Scope

The specific scope of this document is to call out those issues Qualys has uncovered which cannot be resolved with an adjustment to the Qualys scanning engine. A high majority of the time, Qualys is able to avoid such issues and hence they would not appear on our list as systemic problems. Accordingly, the scope of this document is not a comprehensive list of all possible issues a customer could face, but rather a list of issues of which Qualys is currently aware.

Qualys customers scan millions of hosts each month, and there is a wide variance of the age and maintenance of systems. This naturally means new vulnerabilities are discovered on an ongoing basis. A small percentage of these scans uncover previously unknown vulnerabilities, which are typically triggered by a specific sequence of probes sent from the scanner.

Though Qualys may be able to take steps to mitigate the impact, the vulnerability will still exist. As such, a true fix must come from the product vendor. When such issues arise, Qualys Support's express goal is to work closely with you, your internal constituents, and your product vendor to reach resolution.

The following is a list of the known issues we are currently aware of. They are split into two categories. Qualified Reports are issues which Qualys has been able to investigate and determine a root cause. Unqualified Reports are issues which Qualys has not had the opportunity to investigate fully, but have been observed and reported by our customers.

2 Qualified Reports

2.1 Applix TM1

Applix TM1 is a complete application that supports business performance management and operational performance management, including budgeting, forecasting, planning, reporting and analytics.

2.1.1 Applix TM1 – Service Crash

Issue	Applix TM1
Date	4 Nov 2005
Description	Applix TM1 Server, TM1 Admin Server, and the axnet service by default listen on TCP ports 12345, 5495 and 5492, respectively. A remote user may crash these services by connecting to listening ports and sending specific data. Once crashed, the services must be manually restarted in order to regain their normal functionalities.
Products affected	Applix TM1 version 8.4.3 running on Windows 2003 with Service Pack 1 and on Windows XP with Service Pack 2. Note: We have only tested the above version on the above operating systems. Other Applix TM1 versions for the above and other operating systems may also be affected.
Resolution	The vendor has fixed the issues in the latest builds.
Vendor Reference	The vendor did not provide Qualys with a reference number. Details on obtaining updates to the Applix TM1 product are available on the Applix web site at the following URL: http://www.applix.com/

2.2 Candle Roma

Candle Roma is a suite of open message-based computing solutions that support the development, connectivity, and integration of e-business applications.

2.2.1 Candle Roma – Memory Consumption Denial of Service

Issue	Candle Roma
Date	12 Dec 2004
Description	Memory consumption in Candle Roma during a scan consumes 100% resources. Specially, the problem occurs in the common CT component code and affects the krusserv.exe and "kbxapipe.exe" services. This is due to missing packet exception handlers in the Candle application.
Products affected	Candle Roma V3.00 is affected.
Resolution	Candle Roma V3.00 support has ended, and the vendor does not plan to provide any updates/fixes for this version. The problem is fixed in subsequent releases. These releases are not affected: eBP V3.10 (CASP1.0), CASP2.0. It's recommended that you upgrade to the latest release, which is CASP2.0.
Vendor Reference	Please contact IBM/Candle for the latest information by phone at 800-426-7378, or visit the IBM Tivoli support site at this URL: http://www-306.ibm.com/software/sysmgmt/products/support/

2.3 Cisco Products

2.3.1 Cisco Secure ACS – Memory Consumption Denial of Service

Issue	Cisco Secure ACS
Date	16 Aug 2005
Description	Cisco Secure ACS 4.0 has multiple components listening on different TCP ports. Among these, CSAuth listens on TCP port 2000 and CSLog listens on port 2001. These two components do not release resources allocated for TCP connections already terminated by their clients, resulting in handle and memory leaks.

Products affected	Cisco Secure ACS 4.0 running on Windows Server 2003 with Service Pack 1. Note: We have only tested the above version on the above operating system. Other Cisco Secure ACS versions or configurations may also be affected.
Resolution	There is no known fix for this issue.
Vendor Reference	Please visit the Cisco Systems web site for updates to the Cisco Secure ACS product at the following URL: http://www.cisco.com/

2.3.2 CatOS 5.x, 6.x, 7.x, 8.x, 8.xGLX – Denial of Service

Issue	Cisco CatOS
Date	19 Jun 2004
Description	Cisco CatOS is susceptible to a TCP-ACK Denial of Service (DoS) attack on the Telnet, HTTP and SSH service. If exploited, the vulnerability causes the Cisco CatOS running device to stop functioning and reload. A TCP-ACK DoS attack is conducted by not sending the regular final ACK required for a 3-way TCP handshake to complete, and instead sending an invalid response to move the connection to an invalid TCP state. This attack can be initiated from a remote spoofed source. This vulnerability is currently known to be exploitable only if you have the Telnet, HTTP or SSH service configured on a device which is running Cisco CatOS.
Software affected	Cisco CatOS of the following versions are affected: 5.x, 6.x, 7.x, 8.x and 8.xGLX
Products affected	Cisco Catalyst series switches, based on CatOS, of the following series are affected: 29xx, 4xxx, 45xx, 5xxx, 6xxx. Note: Cisco Catalyst series switches that do not use the CatOS are not affected, including but not limited to 1xxx, 3xxx, 8xxx
Resolution	It is recommended that you upgrade to the one of the following CatOS versions or later, depending on your switch series: 5.5 (20), 6.4 (9), 7.6 (6), 8.2 (2), 8.3 (2)GLX

Workaround	For tested workarounds to this issue, please reference the Cisco security advisory, available at the following URL: http://www.cisco.com/warp/public/707/cisco-sa-20040609-catos.shtml
Vendor Reference	Cisco bug IDs: CSCec42751, CSCed45576, and CSCed48590. Cisco security advisory is posted at the following URL: http://www.cisco.com/warp/public/707/cisco-sa-20040609-catos.shtml

---

2.3.3 Cisco CNS Network Registrar – Multiple Vulnerabilities

Issue	Cisco CNS Network Registrar
Date	02 Dec 2004
Description	Normally Cisco CNS Network Register will not crash during a scan, but it might happen after Cisco CNS Network Register is manually restarted a few times without rebooting the host. Cisco CNS Network Registrar DNS/DHCP server for Windows server platforms is vulnerable to a denial of service attack when a specific packet sequence is sent to the server. The referenced Cisco Security Advisory reports two vulnerabilities: CSCeg27625 – The CNS Network Registrar CCM server may consume almost 100% of CPU when a remote user sends a certain sequence of packets and then ends the session. CSCeg27614 – The CNS Network Registrar lock manager process may crash when the system receives an unexpected packet sequence, causing the CCM server to fail.
Products affected	Cisco CNS Network Registrar Versions for Windows NT server and Windows 2000 are affected. For Cisco CSCeg27625, CNS Network Registrar Versions 6.0 through 6.1.1.3 are affected. For Cisco CSCeg27614, all CNS Network Registrar Versions up to and including Version 6.1.1.3 are affected.
Resolution	Vendor has released CNS Network Registrar Version 6.1.1.4 which addresses these issues. Cisco has made free software available to address this vulnerability for all affected customers.
Vendor Reference	Cisco security advisory is available at this URL: http://www.cisco.com/warp/public/707/cisco-sa-20041202-cnr.shtml

2.3.4 Cisco Catalyst 6500 – Host Crash

Issue	Cisco Catalyst 6500 Series switches and routers
Date	07 Oct 2004
Description	Packets sent to the Cisco Catalyst 6500 switch/router on UDP port 500 are not properly handled, leading to memory corruption that sometimes results in crashing the switch/router. Enabling the ISAKMP protocol (UDP port 500) on the switch/router makes it vulnerable to this issue.
Software affected	Cisco IOS 12.1. It's likely that other versions are vulnerable.
Products affected	Cisco Catalyst 6500 Series. Other versions might be vulnerable.
Resolution	Disable ISAKMP (UDP port 500) on the switch/router. To do this, enter "no crypto isakmp enable" from the config mode. As a workaround, you can disable scanning UDP port 500 in Qualys using the profile feature. First create a profile that disables scanning UDP port 500. The easiest method for doing this differs depending on whether the profile will be used for scans, maps or both. Apply the custom profile to each scan or map – on demand or scheduled. (See the online help for complete information on profiles.) For scans, the easiest method is to block port 500 in the Advanced options. Select Blocked Resources, Custom port list, and enter 500 in the field provided. For maps, provide custom UDP port lists in the Advanced options and the Map options. In the Advanced options, configure a custom UDP port list – used during host discovery. And in the Map options, use the Additional field to enter a custom UDP port list – used for information gathering.
Vendor Reference	Cisco bug ID: CSCef59484. For the latest information, log into your CCO account, and use the BugNavigator tool to find the bug details.

2.3.5 Cisco Catalyst 3750X – Denial of Service memory leak

Issue	Cisco Catalyst 3750X memory leak
Date	28 March 2012

Description	Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.
Software affected	Devices configured as a Smart Install client or director are affected by this vulnerability.
Products affected	Cisco Catalyst switches configured as Smart Install client/director.
Resolution	Refer to Cisco Advisory ID: cisco-sa-20120328-smartinstall http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall Cisco has released free software updates that address this vulnerability. A workaround may be available in some versions of Cisco IOS Software if the Smart Install feature is not needed.
Vendor Reference	Advisory ID: cisco-sa-20120328-smartinstall

2.4 Citrix Secured Gateway Service

2.4.1 Secured Gateway Service – DOS/Service Crash

Issue	Citrix Secured Gateway DOS/service crashes when scanned
Date / Qualys Reference	28 Jan 2009 / BID 64993
Description	A vulnerability has been identified in Citrix Secured Gateway Service that could result in a denial of service.
Products affected	This vulnerability is present in all versions of Citrix Secured Gateway up to and including version 3.1. Please note that the Citrix Access Gateway appliance is not affected by this vulnerability when configured to act as a Citrix Secure Gateway.
Resolution	Citrix has an update available that addresses this issue. http://support.citrix.com/article/CTX121172
Vendor Reference	For more information and available fixes, please go to: http://support.citrix.com/article/CTX121172

2.5 CODA Financials

CODA Financials is a financial management software package.

2.5.1 CODA Financials – Denial of Service

Issue	CODA Financials Denial of Service vulnerability
Date / Qualys Reference	17 Apr 2008 / BID 54181
Description	CODA Financials crashes when scanned.
Products affected	CODA Financials v70040418; other versions are possibly affected.
Resolution	Contact CODA support for resolution.
Vendor Reference	N/A

2.6 Computer Associates BrightStor Agent

2.6.1 CA BrightStor Agent – Denial of Service

Issue	CA BrightStor Agent
Date	11 Jan 2006
Description	CA BrightStor's caagentd process listens on TCP port 6051. It is vulnerable to a remote denial of service issue. It can be made unresponsive after a remote user establishes a TCP session to port 6051, sends 7 bytes or less of random data, and terminates the session. Once the process is triggered into a denial of service condition, it has to be manually restarted in order to regain its normal functionality.
Products affected	CA BrightStor version 11.1 running on RedHat 9 with Linux Kernel 2.4.20-8. Note: We have only tested the above version running on the above operating system. Other CA BrightStor versions and configurations may also be affected.
Resolution	There is no known fix for this issue.
Vendor Reference	Please visit the Computer Associates web site for updates to the BrightStor product at this URL: http://www.ca.com/

2.7 Dell SAS RAID Storage Manager

2.7.1 2.14.1 Dell SAS RAID Storage Manager – Service Crash

Issue	Dell SAS RAID Storage Manager (popup.exe)
Date / Qualys Reference	11 Nov 2007 / BID 48813
Description	A component of the Dell SAS RAID Storage Manager – popup.exe – crashes when subjected to a simple SYN scan.
Products affected	popup.exe version 1.0016 – Other versions may be vulnerable as well.
Resolution	Contact Dell with regards to this issue. Qualys is not aware of the vendor's intention to supply a fix for this vulnerability.
Vendor Reference	N/A

2.8 Hewlett-Packard Devices

2.8.1 HP LaserJet M2727NF – Input-Validation

Issue	HP LaserJet input-validation vulnerability
Date / Qualys Reference	24 Jun 2008 / BID 56759
Description	It has been reported that the HP LaserJet M2727NF prints out several pages of "gibberish" when scanned. This seems to be due to a lack of input-validation. Anything sent to ports 8888 and 9999 will be printed out.
Products affected	HP LaserJet M2727NF multi-function devices; similar devices also likely to be affected.
Resolution	Contact HP support for resolution.
Vendor Reference	N/A

2.8.2 HP-UX Portmapper – Denial of Service/Kernel Panic

Issue	HP-UX Portmapper Denial of Service vulnerability
Date / Qualys Reference	08 Aug 2008 / BID 58709

Description	It has been reported that some versions of the Portmapper service (which typically resides on UDP/111) on HP-UX will crash when UDP probes are sent to it.
Products affected	HP-UX 11.31; other versions are possibly affected.
Resolution	HP suggests to update to version B.11.31.08.
Vendor Reference	HP-UX CRID reference QXR1000886293

2.8.3 HP-UX – Host Crash

Issue	HP-UX will experience a host crash
Date / Qualys Reference	21 April 2010 / BID 81388
Description	It has been reported that certain versions of HP-UX below B.11.31.08 may experience a kernel panic during a UDP port scan.
Products affected	Unspecified versions of HP-UX below B.11.31.08.
Resolution	This issue is resolved in HP-UX version B.11.31.08.
Vendor Reference	N/A

2.9 IBM Products

2.9.1 IBM BuildForge Agent Weakness – Host Crash

Issue	IBM BuildForge Agent crashes/exhibits DOS behavior when scanned.
Date / Qualys Reference	20 Feb 2009 / BID 66088
Description	The agent will continuously spawn infinite-looping threads, spiking the CPU and eventually DOSing / crashing the system.
Products affected	BuildForge Agent version 7.0.2
Resolution	IBM has and update available that address this issue. Refer to Vendor Reference.
Vendor Reference	For more information and available fixes please go to: http://www-01.ibm.com/support/docview.wss?uid=swg21303877

2.9.2 IBM Distributed Computing Environment (DCE) – Service Crash

Issue	DCED.exe service crash
Date / Qualys Reference	03 Dec 2007 / BID 49690
Description	IBM's DCE components are installed with various IBM products (e.g., in IBM branded laptops). The DCED.exe service crashes when it receives a particular probe.
Products affected	DCED.exe v.2.2.0.6
Resolution	Contact IBM support for resolution.
Vendor Reference	N/A

2.9.3 IBM Lotus Domino Server – Mail Loop Denial of Service

Issue	IBM Lotus Domino Mail Server
Date	12 Dec 2004
Description	IBM Lotus Domino Mail Server may bounce messages that are generated by mail relay tests and may generate high load/loops in Domino. It's possible for this condition to cause the "Lotus Domino Loop Denial of Service" vulnerability. For more information, refer to this SecuriTeam advisory: http://www.securiteam.com/securitynews/5EP0Y0055Y.html
Products affected	IBM Lotus Domino Server versions 5.0.8 and earlier are affected.
Resolution	Upgrade to Lotus Domino Server version 5.0.9 or greater. Or configure Domino rules to not reply to Qualys mail relay tests and drop them directly. Qualys mail relay tests always use in the source email address the "qgmrfrom" user and "qgmrtest" user. The Qualys external scanner IP ranges are listed in your Qualys account, under Help-> About.
Vendor Reference	Please visit the IBM Lotus support site for the latest information at this URL: http://www-306.ibm.com/software/lotus/support/centers.html

---

2.9.4 IBM Tivoli Storage Manager (TSM) – Service Crash

Issue	IBM Tivoli Storage Manager (TSM)
Date	10 February 2014
Description	IBM Tivoli Storage Manager (TSM) prior to 6.2.4 has been known to crash during port scans.
Products affected	IBM Tivoli Storage Manager (TSM) prior to 6.2.4
Resolution	Upgrade to IBM Tivoli Storage Manager (TSM) prior to 6.2.5 or later.
Vendor Reference	Please visit the IBM Tivoli support site for the latest information at this URL: http://www-947.ibm.com/support/entry/portal/product/tivoli/tivoli_storage_manager?productContext=-2105539168

2.10 Nortel Passport

2.10.1 Nortel Passport 8600 – Denial of Service

Issue	Nortel Passport 8600 DoS
Date	22 Nov 2005
Description	Nortel Passport 8600 switches may be vulnerable to a denial of service issue. This issue can be triggered by starting several concurrent TCP connections to the Nortel Passport web interface (running "RapidLogic" web server) and sending an HTTP request. Once triggered into a denial of service condition, a switch's CPU usage jumps to 100% and the switch stops functioning. The switch must be power cycled to regain normal functionality.
Products affected	Nortel Passport 8600 switches may be affected as well as other Nortel Passport devices.
Resolution	The Qualys Research and Development Team has made updates to the Qualys scanner to avoid scanning Nortel Passport's web interface so that this denial of service will not occur when a Nortel Passport 8600 switch is scanned. However, since we are not aware of the scope of the Nortel devices impacted by this issue, there may still be a potential issue when scanning Nortel devices.
Vendor Reference	Nortel case number: Case 051026-32944

2.11 Novell NetWare

Novell NetWare has **significant security and stability issues** with the use of standard packet forms and protocols, which can cause abends. Novell has released patches for these issues, as referenced in this document.

There are several issues regarding unpatched versions of Novell NetWare that are published on the Novell website as listed below.

NetWare Version 4.1 note: It is a known issue that NetWare V4.1 is vulnerable to port scanning.

Support recommendation: Install the applicable patches from Novell, which have improved the Novell Netware system stability with regards to scanning. These patches are indicated below.

2.11.1 NetWare Version 6.5 – Abend in XNFS/XNFS.NLM

Issue	XNFS.NLM
Date	15 Aug 2003
Description	XNFS.NLM is the NFS Server daemon on NetWare 6.5. The enclosed XNFS.NLM is for use on NetWare 6.5, to prevent a potential abend when Nessus Port Scanner scans a NetWare 6.5 server.
NetWare products affected	NetWare 6.5
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966741.htm
Issue	XNFS
Date	13 Jan 2004
Description	XNFS Abend when accessing invalid ports. Abend in RPCWorker7 Process when Nessus Port Scanner scans a NetWare 6.5 server with invalid ports like: 1234.
Novell products affected	NetWare 6.5
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/10087844.htm

2.11.2 NetWare Version 6.0 – Abend in PKERNEL.NLM

Issue	PKERNEL.NLM
Date	14 Nov 2003
Description	Abend in PKERNEL.NLM when the server is scanned with Nessus. Abend in PKERNEL.NLM, when overflow packet is received. EIP in PKERNEL.NLM at code start +00002D12h.
Novell products affected	NetWare 6.0 NetWare 5.1 Novell NFS Services 3.0 Novell Native File Access for UNIX (NFAU)
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088719.htm
Issue	HTTPSTK.NLM
Date	07 Jul 2003
Description	Abend: EIP in HTTPSTK.NLM at code start +00004CFBh . Performing security scan of NetWare 6 Server causes server to abend in HTTPSTK.NLM.
Novell products affected	NetWare 6.0 Support Pack 2 NetWare 6.0 Support Pack 3
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/10084780.htm
Issue	HTTPSTK Vulnerability Fix - TID2966181
Date	06 JUN 2003
Description	HTTPSTK.NLM to address an Abend in the Netware HTTP Stack caused by a modified keep-alive packet. The Netware HTTP Stack running on Novell Netware 6 (SP3) server ABENDs (abnormal ends) when it receives a modified keep alive packet request on the same TCP connection, which can result in denial of service.
Novell products affected	NetWare 6.0 Service Pack 3
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966181.htm
Issue	BTCPCOM
Date	11 Jul 2003

Description	BTCPCOM CPU Hog ABEND Fix. There is a possibility of a CPU Hog Timeout ABEND in BTCPCOM.NLM when running a port scanning utility against a NetWare server.
Novell products affected	NetWare 6.0 NetWare 5.1
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966492.htm

2.11.3 NetWare Version 5.1 – Abend in PKERNEL.NLM

Issue	PKERNEL.NLM
Date	14 Nov 2003
Description	1) Abend in PKERNEL.NLM when the server is scanned with Nessus, a security scanner tool. 2) Abend in PKERNEL.NLM, when overflow packet is received. 3) EIP in PKERNEL.NLM at code start +00002D12h.
Novell products affected	NetWare 6.0 NetWare 5.1 Novell NFS Services 3.0 Novell Native File Access for UNIX (NFAU)
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/10088719.htm
Issue	BTCPCOM
Date	11 Jul 2003
Description	BTCPCOM CPU Hog ABEND Fix. There is a possibility of a CPU Hog Timeout ABEND in BTCPCOM.NLM when running a port scanning utility against a NetWare server.
Novell products affected	NetWare 6.0 NetWare 5.1
Vendor Reference	http://support.novell.com/cgi-bin/search/searchtid.cgi?/2966492.htm

2.12 Oracle Cluster Synchronization Services

Oracle Cluster Synchronization Services (OCSSD) is a component of Oracle Cluster Ready Services (CRS), which is included in Oracle10g.

2.12.1 Oracle Cluster Synchronization Services – Denial of Service

Issue	Oracle Cluster Synchronization Services
Date	16 Nov 2005
Description	The OCSSD process listens on a dynamic port. When a remote attacker connects to the OCSSD's listening port and sends 0, 1, 2, or 3 bytes of data before terminating the connection, the OCSSD process fails to free the socket it acquired for the connection. Since there is a limit on the number of file descriptors a process can own, the remote attacker may repeat the above process until OCSSD exhausts the maximum number of file descriptors and stops accepting new connections. Once triggered into this denial of service condition, the OCSSD process must be manually restarted to regain its normal functionality.
Products affected	Oracle Cluster Synchronization Services (OCSSD) in Oracle 10g (versions 10.1.0.4 and 10.1.0.3) running on Windows 2003 and RedHat AS3. Note: We have only tested the above versions on the above operating systems. Other Oracle OCSSD versions for the above and other operating systems may also be affected.
Resolution	There is no known fix for this issue.
Vendor Reference	Please visit the Oracle web site for updates to Oracle's database products at the following URL: http://www.oracle.com/

2.13 Oracle COREid Access Server

Oracle COREid Access and Identity delivers critical functionality for access control, single sign- on, and user profile management.

2.13.1 Oracle COREid Access Server – CPU Utilization Denial of Service

Issue	Oracle COREid Access Server
Date	15 Aug 2005

Description	Oracle COREid Access Server listens on TCP port 6021. When a remote user connects to this port, sends specially crafted data, and keeps the connection alive, the COREid Access Server utilizes almost 100% CPU.
Products affected	Oracle COREid Access Server version 6.11.18 running on AIX 5.1. Note: We have only tested the above version on the above operating system. Other Oracle COREid Access Server versions or configurations may also be affected.
Resolution	There is no known fix for this issue.
Vendor Reference	Please visit the Oracle web site for updates to the COREid Access Server product at the following URL: http://www.oracle.com/

2.14 Polycom SoundPoint

The Polycom SoundPoint is a series of VoIP phones.

2.14.1 Polycom SoundPoint IP 330 SIP – Denial of Service

Issue	Polycom SoundPoint IP 330 SIP Denial of Service
Date / Qualys Reference	16 July 2008 / BID 57777
Description	The Polycom SoundPoint IP 330 VoIP phone is vulnerable to a Denial-of-Service condition. The device reboots when scanned.
Products affected	Polycom SoundPoint IP 330 SIP; similar devices also likely to be affected.
Resolution	There is no known fix for this issue.
Vendor Reference	N/A

2.15 Sybase Adaptive Server Enterprise (ASE)

Adaptive Server Enterprise (ASE) is Sybase Corporation's (Now SAP AG) flagship enterprise-class relational model database server product. ASE is predominantly used on the Unix platform but is also available for Windows.

2.15.1 Sybase ASE - CPU Utilization Denial of Service

Issue	Sybase ASE crash
Date / Qualys Reference	1 January 2011 / BID 98402

Description	Sybase ASE server crashes due to high CPU utilization.
Products affected	Sybase ASE versions 12.5.3 and 12.5.4 on SunOS
Resolution	Sybase recommends excluding ASE ports from scanning.
Vendor Reference	Sybase CR 635047.

2.16 TIDAL Agent

TIDAL Agent is enterprise software provided by TIDAL Software, a provider of enterprise management and automation tools for the enterprise.

2.16.1 TIDAL Agent – Denial of Service

Issue	TIDAL Agent (Agent.exe, file version 2.0.0.8)
Date	09 Sep 2005
Description	TIDAL Agent is vulnerable to a Denial of Service condition. TIDAL Agents listen on user-configurable TCP ports. By default, the first TIDAL Agent listens on TCP port 5912, the second on TCP port 5913, and so on. When a remote user connects to a TIDAL Agent's listening port, sends a few (e.g. 3) bytes of random data, terminates the connection, and then repeats this process for five additional times, this TIDAL Agent stops responding to any new connection requests. Once triggered into this denial of service condition, it does not seem possible to restart the TIDAL Agent without rebooting the host.
Products affected	TIDAL Agent (Agent.exe, file version 2.0.0.8) running on Windows 2000 with Service Pack 4. It's likely that other operating systems are affected.
Resolution	TIDAL software is aware of this issue. Please contact TIDAL Software for the latest information and updates: http://www.tidalsoft.com/
Vendor Reference	The TIDAL Software reference ID for this issue is SR#26028.

3 Unqualified Reports

3.1 Blue Coat Director

Blue Coat Director enables you to centrally manage network policies and devices from a single, easy-to-use Web interface. With Director, IT administrators can automatically deploy hundreds of appliances, monitor and enforce security policies and respond to emergencies with the click of a button. Director also allows you to automatically respond to sudden changes in the network, including disasters and outages, so you can fix them before they impact the end user.

3.1.1 Blue Coat Director – Host Crash

Issue	Blue Coat Director host crash
Date / Qualys Bug ID	27 May 2009 / BID 71096
Description	Blue Coat Director server caused the system to crash when scanning. Issue has been isolated to HTTP traffic being sent to the device during a scan.
Products affected	Blue Coat Director versions 4.2.2.2
Resolution	A mitigation option of placing the director behind a firewall and blocking HTTP traffic. Update to a later version of Blue Coat Director.
Vendor Reference	N/A

3.2 Brocade Fabric OS

Brocade Fabric OS is operating system firmware that provides core infrastructure for deploying Storage Area Networks (SANS) in enterprise environments. Fabric OS is embedded in Brocade Silkworm switches as well as switches manufactured by third party vendors.

3.2.1 Brocade Fabric OS – Memory Consumption Denial of Service

Issue	Brocade Fabric Series 2 and 3 OS firmware
Date	24 May 2004
Description	There are issues with security and management software that polls switches embedded with Brocade Fabric OS. Reportedly, requests are accumulated and not cleaned up properly in the switch memory, and there are a few memory leak issues. The latest firmware resolves these issues.

Products affected	Switches based on Brocade Fabric OS Version 3.0.2f and earlier are affected, such as Brocade Silkworm switches and EMC Connectrix DS-16B2. Some Silkworm V2.x and V3.x switches are affected. Note: Silkworm switches using Fabric OS V4.x are not affected, including SW3900, SW12000, SW24000, SW3250, and SW3850.
Resolution	It is recommended that you upgrade to the latest firmware level, which fixes several memory leak issues. For Silkworm V2.x switches, upgrade to Fabric OS V2.6.2 or later. For Silkworm V3.x switches using Fabric OS V3.x, upgrade to Fabric OS V3.1.2 or later.
Vendor Reference	For more information on this known issue, customers can obtain Release Notes Revision 3.1.2 from the equipment provider.

3.3 Cisco 3640

The Cisco 3640 modular access routers are based on the Cisco 3600 multifunction platform which supports hybrid dial applications, LAN-to-LAN or routing applications, and multiservice applications. The Cisco 3640 router is equipped with four network module slots, allowing integration with over 70 network modules and interfaces.

3.3.1 Cisco 3640 – Denial of Service

Issue	Cisco 3640 router
Date	17 May 2004
Description	Scanning a C class network with more than 30 hosts behind it will bounce the Cisco 3640 router interface.
Software affected	Cisco Internetwork Operation System Software IOS™ 3600 Software (C3640-IK9S-M), Version 12.2(16f), RELEASE SOFTWARE (fc1) Copyright © 1986-2004 by Cisco Systems, Inc.

Products affected	Cisco 3640 (R4700) processor (revision 0x00) with 98304K/32768K bytes of memory. Processor board ID 27612296 R4700 CPU at 100Mhz, Implementation 33, Rev 1.0 Bridging software. X.25 software, Version 3.0.0. SuperLAT software (© 1990 by Meridian Technology Corp). 4 Ethernet/IEEE 802.3 interface(s) 2 FastEthernet/IEEE 802.3 interface(s) 1 Serial network interface(s) DRAM configuration is 64 bits wide with parity disabled. 125K bytes of non-volatile configuration memory. 32768K bytes of processor board System flash (Read/Write) ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1) ROM: 3600 Software (C3640-IK9S-M), Version 12.2(16b), RELEASE SOFTWARE (fc1) System image file is "flash:c3640-ik9s-mz.122-16f.bin"
Resolution	Do not scan an entire class C. Scan router by itself.
Vendor Reference	N/A

3.4 Citrix

3.4.1 Citrix Access Gateway

Issue	Service Crash
Date / Qualys Reference	12 Oct 2009 / BID 75820
Description	It has been reported that Citrix Access Gateway Standard Edition 4.5.5 build 45 may crash when being scanned. Qualys has narrowed the cause down to a particular request. ---[code]--- GET ftp://89.167.157.104/~<img%20src=”test”%20onclick=”alert(‘XSS’)”> HTTP/1.0\r\n\r\n ---[code]---
Products affected	Citrix Access Gateway Standard Edition 4.5.5 build 45 (others may be affected as well)

Resolution	Qualys has implemented a modification to avoid service impact. Qualys is not aware of a vendor fix to this vulnerability.
Vendor Reference	N/A

3.5 EMC

3.5.1 EMC EmailXtender – Service Crash

Issue	Multiple service crash
Date / Qualys Reference	03 Dec 2007 / BID 49671
Description	Multiple services related to EMC EmailXtender appear to lack robust error handling when accepting data from a remote host. It is possible to crash the following services remotely: exHealthCheck.exe, exQuery.exe, exMail.exe, and exAdmin.exe.
Products affected	EMC EmailXtender 4.8 Patch 266. Other versions may be vulnerable as well.
Resolution	Qualys is unaware of a vendor patch.
Vendor Reference	N/A

3.5.2 EMC Master Agent – Service Crash

Issue	MNRAgent.exe service crash
Date / Qualys Reference	14 Nov 2007 / BID 49665
Description	MNRAgent.exe – the EMC Master Agent – crashes when scanned.
Products affected	EMC Master Agent (MNRAgent.exe) – version unknown.
Resolution	It has been reported that the newest versions don't crash. Please contact the vendor for further information.
Vendor Reference	N/A

3.6 Fujitsu

3.6.1 Fujitsu System Management Board – Service Crash

Issue	Fujitsu System Management Board
Date / Qualys Reference	28 Apr 2016 / BID 17392
Description	Fujitsu System Management Board Crashes During Qualys Scan
Products affected	SDR 3.13 ID 0493 RX4770M2 Firmware 7.84F (1.00) SDR 3.16 ID 0493 RX4770M2 Firmware 8.05F (1.00) SDR 3.16 ID 0493 RX4770M2 Firmware 8.08F (1.00) SDR 3.41 ID 0443 RX4770M1 Firmware 7.84F (1.00) SDR 3.43 ID 0443 RX4770M1 Firmware 8.08F (1.00) SDR 3.59 ID 0416 RX2540M1 Firmware 7.82F (1.00) SDR 3.64 ID 0416 RX2540M1 Firmware 8.05F (1.00) SDR 3.71 ID 0356 RX300S8 Firmware 7.82F (1.00) SDR 3.71 ID 0356 RX300S8 Firmware 8.05F (1.00)
Resolution	Qualys is unaware of a vendor patch. The following versions are not affected: SDRR 3.03 ID 0278 RX600S6 SDRR 3.15 ID 0263 RX300S6 SDRR 3.19 ID 0317 RX500S7 SDRR 3.24 ID 0258 RX600S5 SDRR 3.25 ID 0258 RX600S5 SDRR 3.27 ID 0316 RX300S7
Vendor Reference	N/A

3.7 IBM Remote Supervisor Adapter

3.7.1 IBM Remote Supervisor Adapter – Service Crash

Issue	IBM RSA multiple service crash
Date / Qualys Reference	08 Feb 2007 / BID 41551
Description	IBM Remote Supervisor Adapters contain web and telnet services that crash when scanned.
Products affected	IBM RSAs – version unknown
Resolution	It has been reported that the newest versions don't crash. Please contact the vendor for further information.
Vendor Reference	N/A

3.8 NEC projector LT265

3.8.1 NEC projector LT265 – Device becomes unresponsive

Issue	NEC projector LT265 series becomes unresponsive scan.
Date / Qualys Reference	01 Aug 2008 / BID 69533
Description	Device does not respond to remote control, and buttons on front of device also become unresponsive when scanned.
Products affected	NEC projector LT265 series
Resolution	Qualys is unaware of a vendor patch.
Vendor Reference	N/A

3.9 Netopia Caymon 3546

Netopia Caymon 3546 ADSL Gateway combines an ADSL modem and router with a 10/100Base-TX switch to enable broadband connection for SOHO and small business networks.

3.9.1 Netopia Caymon 3546 – Host Crash

Issue	Netopia Caymon 3546 host crash
Date	28 Feb 2005
Description	Netopia Caymon 3546 router crashes during a scan.
Products affected	Netopia Caymon 3546 router with firmware 6.4.0.R2. Earlier firmware versions may be affected as well.
Resolution	There will be no further upgrades to Netopia Caymon 3546. Vendor recommends upgrading to Netopia Caymon 3346N router and enabling Stateful Inspection.
Vendor Reference	Read about Stateful Inspection in the “3300 Series User Guide version 7.4,” which is available from this URL: http://netopia.com/en-us/equipment/tech/doc_center.html

---

3.10 NetScaler

NetScaler Application Delivery Systems provide a solution for optimized delivery of applications, while ensuring continuous availability of applications and content.

3.10.1 NetScaler Load Balancer – Host Crash

Issue	NetScaler Load Balancer host crash
Date	10 Jun 2004
Description	NetScaler Load Balancer crashes during a scan.
Products affected	NetScaler Load Balancer versions 5.2.50.8 and earlier as well as versions 6.0.47.6 and earlier are affected.
Resolution	Vendor has addressed this issue in NetScaler versions 5.2.50.9 and 6.0.47.7. If you are running an affected version, upgrade to the latest version. For more information, contact NetScaler Technical Support by phone at 1-866-NETSCALER or via email at support@netscaler.com.
Vendor Reference	N/A

3.11 Nortel Switches 4500 and 5500 Series

3.11.1 Nortel Switch – Host Crash

Issue	Nortel 4500 and 5500 series switches crash when scanned
Date / Qualys Reference	06 Mar 2009 / BID 66802
Description	Nortel switch device actually reboots when scanned.
Products affected	Nortel 4550T PWR, 5510-48T, 5520-24T-PWR. Other versions may be vulnerable as well.
Resolution	Qualys is unaware of a vendor patch.
Vendor Reference	N/A

3.12 Oracle Rdb

The Oracle Rdb product family includes Oracle Rdb Enterprise Edition, Oracle CODASYL DBMS, Oracle CDD/Repository, Oracle SQL/Services, OCI Services for Oracle Rdb, Oracle Trace for Rdb, Replication Option for Rdb, Oracle Rdb ODBC Driver, and Oracle Rdb JDBC Drivers. For more information, visit http://www.oracle.com/rdb.

3.12.1 Oracle Rdb – Denial of Service

Issue	Unknown DoS condition
Date	N/A
Description	The Oracle Rdb database server is vulnerable to a Denial of Service condition
Products affected	Oracle Rdb 7.0 and 7.1 running under OpenVMS. Note that this is not the Oracle RDBMS system, but the former DEC Rdb that is affected.
Resolution	This issue has been fixed in Oracle Rdb version 7.2, current version is 7.2.1
Vendor Reference	N/A

3.13 Red Hat Enterprise Linux

Red Hat Enterprise Linux (RHEL) is a Linux-based operating system developed by Red Hat and targeted toward the commercial market. For more info visit http://www.redhat.com/products/enterprise-linux/server/

3.13.1 RHEL Dual NIC – Kernel Panic

Issue	Kernel panic causes server reboot
Date / Qualys Reference	01 Jan 2013 / CRM 717811
Description	The issue is caused by skb_gro_header_slow parameter which unconditionally resets frag0 and frag0_len in the configured network device. However when this skb can't be pulled on, this leaves the GRO fields in an inconsistent state. When NAPI_GRO_CB(skb)->frag0 is dereferenced, the kernel panics with a NULL pointer dereference.
Products affected	Dual NIC Server using RHEL 5.6 kernel 2.6.18-238.9.1 and RHEL 5.5 kernel 2.6.18-194.11.4
Resolution	Customer reported this RHEL Bug 726552
Vendor Reference	https://bugzilla.redhat.com/show_bug.cgi?format=multiple&id=726552

3.14 SAP Netweaver

3.14.1 SAP Netweaver – Service Crash

Issue	icman service crash
Date / Qualys Reference	07 Dec 2007 / BID 49878
Description	The Internet Communication Manager (icman) component of SAP Netweaver appears to lack robust error handling when accepting data from a remote host. It is possible to crash the service remotely.
Products affected	SAP NetWeaver 7.0 patch level 94 – Other versions may be vulnerable as well.
Resolution	Qualys is unaware of a vendor patch.
Vendor Reference	N/A

3.15 Sun Applications

3.15.1 Sun Forte Developer

Issue	Sun Forte Developer service crash
Date / Qualys Reference	12 Jan 2010 / BID 77546
Description	It has been reported that Sun Forte Developer 5.2.34 may crash during a scan.
Products affected	Sun Forte Developer 5.2.34 (other versions may be affected as well)
Resolution	Qualys is not aware of a vendor solution, however, Sun Forte Developer has deprecated in favor of Sun ONE studio. Please contact the vendor for specific information surrounding Sun ONE.
Vendor Reference	N/A

3.16 VMWare ESX Server

3.16.1 VMWare ESX Server – Service Crash

Issue	VMWare ESX hostd crash
Date / Qualys Reference	01 Feb 2008 / BID 51339
Description	The hostd service in VMWare ESX server crashes when scanned.
Products affected	VMWare ESX Server v.3.01 and 3.02
Resolution	VMWare fixed the 3.01 crash with the release of 3.02. 3.02 is still vulnerable, but a workaround in the Qualys scan engine mitigates the crash.
Vendor Reference	N/A

3.17 Websense

3.17.1 Websense Reporter – Service Crash

Issue	ExplorerServer.exe service crash
Date	03 Jan 2008
Description	ExplorerServer.exe, the web-server interface to the Websense reporting engine, crashes when scanned.
Products affected	Websense Reporter v.5.5; ExplorerServer.exe v.5.5.0.161 – Other versions may be vulnerable as well.
Resolution	Websense has reportedly fixed this vulnerability in a later version.
Vendor Reference	N/A

3.18 Xerox DC405 Printer

3.18.1 Xerox DC405 Printer – Excessive Network Traffic

Issue	Unknown DoS condition
Date / Qualys Reference	26 Nov 2007 / BID 49349
Description	Scanning this device may cause it to enter into a partially functional state. In this state, the printer will reportedly continue sending ACKs to the Qualys scanner, even after the scan has completed. In maintaining RFC compliance, the Qualys scanner will send RST packets for every unsolicited ACK. The net effect may lead to a network level denial of service.
Products affected	Xerox DC405 printers. Other models may be affected as well.
Resolution	Qualys is unaware of a vendor patch.
Vendor Reference	N/A