PULSE SECURE PRODUCT RELEASE NOTES

PRODUCT: STINGRAY TRAFFIC MANAGER

RELEASE DATE: 13TH DECEMBER, 2017

VERSION: 9.9R3

CONTENTS

1) ABOUT THIS RELEASE

Stingray Traffic Manager 9.9r3 is a minor revision of the Stingray product family, containing a number of bug fixes. Customers are recommended to upgrade to this version to take advantage of the changes.

2) PLATFORM AVAILABILITY

- Linux x86_64: Kernel 2.6.18 – 3.19 (2.6.22+ for IPv6), glibc 2.5+

- Solaris 10 (x86_64)
- Virtual Appliances:
  - VMware vSphere 5.5, 6.0;
  - XenServer 6.2, 6.5;
  - Oracle VM for x86 3.2, 3.3;
  - Microsoft Hyper-V Server 2012 & 2012 R2;
  - Microsoft Hyper-V under Windows Server 2012 & 2012 R2;
  - QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 14.04, 16.04);

  NOTE: VMware virtual appliances are now solely deployed through OVF packages.
- Amazon EC2 - as a virtual appliance or native software install

3) RESOURCE REQUIREMENTS

Virtual appliances should be allocated a minimum of 2 GB of RAM.

4) UPGRADING FROM 9.9, 9.9R1, OR 9.9R2

Please refer to the "Known Issues in 9.9r3" section in this document before the upgrade.

5) CHANGES IN 9.9R3

Installation and Upgrading

- **VTM-36991** Fixed a value encoding issue on the 'System > Traffic Managers' page of the Admin UI.
- **VTM-32072** The initial size of the disk image file for the KVM virtual appliance has been reduced.
- **VTM-33527** Fixed an issue for traffic manager appliances deployed on Citrix XenServer 7.0 whereby the appliance would incorrectly continue to use the current partition after a post-upgrade reboot but attempt to use the updated kernel version, resulting in an unusable state. Before upgrading appliances older than 17.1, the "PV-legacy-args" VM parameter should be removed using the following command on the XenServer host: "xe vm-param-set uuid=[VM UUID] PV-legacy-args"
- **VTM-32253** Fixed a problem whereby some warnings from a successful upgrade were not reported in the logs.

Configuration

- **VTM-32387** A fix has been made to the backup comparison mechanism to correctly categorize 'locations.cfg' and 'appliance/nat.cfg', in order to output the timestamps of the differing files.

Administration Server

- **VTM-36984** Fixed a value encoding issue in the Sysctl page of the Admin UI on appliances.
- **VTM-34076** Explicit upgrade of group permissions for new features has been added to the traffic manager, and is applied retroactively back to version 7.2. In most cases a safe default of 'No Access' is set for new permissions added by a feature. Note that as a result of this change, features to which non-admin users previously had 'Read-Only' access might no longer be accessible. A suitably privileged administrator can update group permissions to restore access for affected users.
- **VTM-23643**, **SR31188** Added the 'HttpOnly' property to the session cookie that provides authenticated access to the Admin UI.
- **VTM-36864** Fixed an issue where any authenticated user logged into the Admin UI could access images of historical activity graphs.
- **VTM-36292** Improved the security of internal communication channels used between the traffic manager and the applet of the administrative server.
- **VTM-35507** The expat XML parser library included in the administration server has been updated to version 2.2.3 to fix the security vulnerabilities CVE-2017-9233 and CVE-2016-9063.
- **VTM-35328** The version of Perl bundled with the traffic manager has been patched to address CVE-2017-6512.
- **VTM-21327**, **VTM-24942**, **VTM-22116**, **SR27556**, **SR34209**, **SR28872** When upgrading a cluster of traffic managers, a new configuration key might be added to the configuration of the upgraded traffic managers. This configuration change could previously have resulted in the virtual server displaying an error state on the front page of the Administration Server due to the configurations being slightly different between the machines that have and have not been upgraded. The service will no longer display an error condition if the configuration files differ until all traffic managers have been upgraded.

Authentication

- **VTM-36924** Added a warning to the user permission groups page that some permission settings give the ability to run scripts with the same UNIX user permissions as the traffic manager, and should be treated with caution. For more details see the 'Permission Groups' section of the User's Guide.
- **VTM-36271** Passwordless login for local ZCLI command execution now uses a dedicated transient secret protected by filesystem ACLs.

REST API

- **VTM-37048** Fixed an issue where a REST request for a resource protected by a group sub permission could be incorrectly granted PUT / GET access even though the permission was set to "none". For example, if SSL!Client_Keys was "none" and SSL was "ro" then REST would incorrectly permit and respond to GET requests for /config/active/ssl/client_keys.
- **VTM-36296** Improved the security of REST API proxied statistics requests. As a result of this change, traffic managers running versions from 17.4, 17.2r1, 10.4r2 or 9.9r3 onwards will be unable to proxy REST API requests to traffic managers without this improvement.

ZCLI

- **VTM-36021** Fixed an issue where the zcli command would fail to connect when the combined length of the username and password exceeded 56 characters.

SNMP

- **VTM-34396** Fixed the SNMPv1 MIB to be compliant with SMI standards.

TrafficScript

- **VTM-35385** The libxml2 XML parser library has been patched to fix CVE-2017-9047, CVE-2017-9048, CVE-2017-9049 and CVE-2017-9050.
- **VTM-34491** The fix for CVE-2017-5029 was applied to the libxslt 1.1.29 software incorporated into the traffic manager.
- **VTM-34610** The libxml2 XML parser library has been patched to fix CVE-2016-4658 and CVE-2016-5131. CVE-2016-4448 was fixed when libxml2 was updated to version 2.9.4 in a previous release.

Connection Processing

- **VTM-35864**, **VTM-35975** Fixed an issue where a 'DNS (UDP)' or 'DNS (TCP)' virtual server would incorrectly respond to queries for new DNS Resource Record types such as CAA (Certification Authority Authorization) with a 'REFUSED' error rather than allowing the request through to a back-end node.

Bandwidth Management

- **VTM-21912**, **VTM-36372**, **VTM-23011**, **SR28529**, **SR30135** Fixed an issue where a traffic manager child process that had been restarted after unexpectedly terminating could have failed to process new connections, resulting in them stalling indefinitely.

Health Monitoring

- **VTM-34078** Fixed an issue that could cause pool monitors to occasionally fail to update a node's health status. These failures were transient - the monitor would correctly update the node's state when it next performed a health check.

Global Load Balancing

- **VTM-26188** Fixed an issue where the traffic manager needed a restart in order for the GLB feature to use user-specified geo-location entries.

DNS Server

- **VTM-36693** Fixed a value encoding issue in the DNS Zones Files catalog page of the Admin UI.

SSL/TLS and Cryptography

- **VTM-36744**, **VTM-34086** The library modified from OpenSSL that is used by the traffic manager has been upgraded to version 1.0.2m, addressing CVE-2017-3732 and CVE-2017-3736. This library is used to provide cryptographic primitives such as RSA or AES.
- **VTM-36247** Improved the security of internal communication channels used between traffic manager processes.
- **VTM-35553**, **VTM-18863**, **VTM-7378**, **SR23577**, **SR10791** Integrated support for the Thales nShield product family has been removed from traffic manager appliances. The capability to install, configure and use nShield Connect products remains an option through the use of the generic PKCS#11 SSL Hardware capability and the Open Access VA policy. Warning: Upgrading to this release will remove all security worlds that were managed by the traffic manager in appliances created using previous releases. As a result all keys protected by those security worlds will no longer be usable, meaning SSL decrypting virtual servers using SSL/TLS certificates based upon those keys will no longer be able to create new connections. There is a similar impact for client certificates used to authenticate the traffic manager to pool nodes. Administrators using the integrated support for Thales nShield products, wanting to upgrade a traffic manager cluster to this release, should do so with a plan that includes the deployment of support software for their HSM hardware, along with the creation of new SSL/TLS certificates where hardware protected keys are required.

Logging

- **VTM-23984**, **VTM-23985**, **SR31922**, **SR31923** When changing a secret via the REST API the value of the secret will be audit logged as a row of asterisks.

Web Accelerator

- **VTM-34387** When parsing a quoted section, the CSS parser would interpret parenthesis as part of the document instead of a literal, resulting in a corrupted CSS document. Parenthesis are now ignored inside string literals.
- **VTM-33571** Web Accelerator no longer serves WebP images to Microsoft Edge browsers, which do not support that image format.
- **VTM-33607** Updated libpng to version 1.2.57, which fixes CVE-2016-10087

Pool Autoscaling

- **VTM-35649**, **VTM-36290** Fixed an issue that caused DNS-derived autoscaling to not add a node back into a pool if that node had previously been removed from the pool and was marked as having failed by a health monitor at the time it was removed.
- **VTM-34349**, **VTM-35445**, **VTM-35172**, **VTM-33978**, **VTM-21562**, **SR28019** Fixed an issue where the autoscaler process could stop unexpectedly when autoscaling was disabled on a pool.
- **VTM-29565**, **SR28454** Fixed an issue whereby changing a clusters license support for autoscalling or analytics caused log events equal to the number of vTM child processes instead of only a single event

6) STINGRAY TRAFFIC MANAGER APPLIANCE

Appliance OS

- **VTM-36810** Updated the appliance kernel to version 3.13.0-135.184, and updated packages installed on the appliance. These updates include changes addressing:

CVE-2014-8501 CVE-2014-9900 CVE-2014-9911 CVE-2014-9939 CVE-2014-9940
CVE-2015-4844 CVE-2015-7554 CVE-2015-8270 CVE-2015-8271 CVE-2015-8272
CVE-2015-8668 CVE-2015-8709 CVE-2015-8944 CVE-2015-8955 CVE-2015-8962
CVE-2015-8963 CVE-2015-8964 CVE-2015-8966 CVE-2015-8967 CVE-2015-8982
CVE-2015-8983 CVE-2015-8984 CVE-2016-0494 CVE-2016-0634 CVE-2016-0772
CVE-2016-1234 CVE-2016-1248 CVE-2016-1252 CVE-2016-1867 CVE-2016-2089
CVE-2016-2177 CVE-2016-2183 CVE-2016-2226 CVE-2016-3622 CVE-2016-3623
CVE-2016-3624 CVE-2016-3632 CVE-2016-3658 CVE-2016-3706 CVE-2016-3945
CVE-2016-3990 CVE-2016-3991 CVE-2016-4429 CVE-2016-4448 CVE-2016-4487
CVE-2016-4488 CVE-2016-4489 CVE-2016-4490 CVE-2016-4491 CVE-2016-4492
CVE-2016-4493 CVE-2016-4658 CVE-2016-5131 CVE-2016-5285 CVE-2016-5314
CVE-2016-5315 CVE-2016-5316 CVE-2016-5317 CVE-2016-5320 CVE-2016-5321
CVE-2016-5322 CVE-2016-5323 CVE-2016-5546 CVE-2016-5547 CVE-2016-5548
CVE-2016-5552 CVE-2016-5636 CVE-2016-5652 CVE-2016-5699 CVE-2016-5875
CVE-2016-6131 CVE-2016-6213 CVE-2016-6223 CVE-2016-6252 CVE-2016-6293
CVE-2016-6321 CVE-2016-6323 CVE-2016-7056 CVE-2016-7097 CVE-2016-7098
CVE-2016-7415 CVE-2016-7425 CVE-2016-7426 CVE-2016-7427 CVE-2016-7428
CVE-2016-7429 CVE-2016-7543 CVE-2016-7910 CVE-2016-7911 CVE-2016-7914
CVE-2016-7916 CVE-2016-7922 CVE-2016-7923 CVE-2016-7924 CVE-2016-7925
CVE-2016-7926 CVE-2016-7927 CVE-2016-7928 CVE-2016-7929 CVE-2016-7930
CVE-2016-7931 CVE-2016-7932 CVE-2016-7933 CVE-2016-7934 CVE-2016-7935
CVE-2016-7936 CVE-2016-7937 CVE-2016-7938 CVE-2017-7939 CVE-2016-7940
CVE-2016-7973 CVE-2016-7974 CVE-2016-7975 CVE-2016-7983 CVE-2016-7984
CVE-2016-7985 CVE-2016-7986 CVE-2016-7992 CVE-2016-7993 CVE-2016-8331
CVE-2016-8405 CVE-2016-8574 CVE-2016-8575 CVE-2016-8610 CVE-2016-8632
CVE-2016-8633 CVE-2016-8635 CVE-2016-8645 CVE-2016-8650 CVE-2016-8654
CVE-2016-8655 CVE-2016-8658 CVE-2016-8691 CVE-2016-8692 CVE-2016-8693
CVE-2016-8882 CVE-2016-9074 CVE-2016-9083 CVE-2016-9084 CVE-2016-9131
CVE-2016-9147 CVE-2016-9178 CVE-2016-9191 CVE-2016-9273 CVE-2016-9297
CVE-2016-9310 CVE-2016-9311 CVE-2016-9401 CVE-2016-9427 CVE-2016-9444
CVE-2016-9448 CVE-2016-9453 CVE-2016-9532 CVE-2016-9533 CVE-2016-9534
CVE-2016-9535 CVE-2016-9536 CVE-2016-9537 CVE-2016-9538 CVE-2016-9539
CVE-2016-9540 CVE-2016-9555 CVE-2016-9560 CVE-2016-9586 CVE-2016-9591
CVE-2016-9604 CVE-2016-9754 CVE-2016-9756 CVE-2016-9793 CVE-2016-9794
CVE-2016-9806 CVE-2016-10044 CVE-2016-10088 CVE-2016-10092
CVE-2016-10093 CVE-2016-10094 CVE-2016-10109 CVE-2016-10200
CVE-2016-10244 CVE-2016-10249 CVE-2016-10251 CVE-2016-10328
CVE-2016-1000110 CVE-2017-0605 CVE-2017-0663 CVE-2017-2616

CVE-2017-2618 CVE-2017-2636 CVE-2017-2862 CVE-2017-2870 CVE-2017-3135
CVE-2017-3136 CVE-2017-3137 CVE-2017-3138 CVE-2017-3142 CVE-2017-3143
CVE-2017-3231 CVE-2017-3238 CVE-2017-3241 CVE-2017-3243 CVE-2017-3244
CVE-2017-3252 CVE-2017-3253 CVE-2017-3258 CVE-2017-3261 CVE-2017-3265
CVE-2017-3272 CVE-2017-3289 CVE-2017-3291 CVE-2017-3302 CVE-2017-3305
CVE-2017-3308 CVE-2017-3309 CVE-2017-3312 CVE-2017-3313 CVE-2017-3317
CVE-2017-3318 CVE-2017-3329 CVE-2017-3453 CVE-2017-3456 CVE-2017-3461
CVE-2017-3462 CVE-2017-3463 CVE-2017-3464 CVE-2017-3509 CVE-2017-3511
CVE-2017-3526 CVE-2017-3533 CVE-2017-3539 CVE-2017-3544 CVE-2017-3600
CVE-2017-3635 CVE-2017-3636 CVE-2017-3641 CVE-2017-3648 CVE-2017-3651
CVE-2017-3652 CVE-2017-3653 CVE-2017-3731 CVE-2017-3735 CVE-2017-5202
CVE-2017-5203 CVE-2017-5204 CVE-2017-5205 CVE-2017-5225 CVE-2017-5335
CVE-2017-5336 CVE-2017-5337 CVE-2017-5341 CVE-2017-5342 CVE-2017-5461
CVE-2017-5462 CVE-2017-5482 CVE-2017-5483 CVE-2017-5484 CVE-2017-5485
CVE-2017-5486 CVE-2017-5970 CVE-2017-5986 CVE-2017-6074 CVE-2017-6214
CVE-2017-6311 CVE-2017-6346 CVE-2017-6458 CVE-2017-6462 CVE-2017-6463
CVE-2017-6464 CVE-2017-6508 CVE-2017-6891 CVE-2017-6951 CVE-2017-6964
CVE-2017-7184 CVE-2017-7187 CVE-2017-7261 CVE-2017-7273 CVE-2017-7294
CVE-2017-7308 CVE-2017-7346 CVE-2017-7375 CVE-2017-7376 CVE-2017-7407
CVE-2017-7472 CVE-2017-7482 CVE-2017-7487 CVE-2017-7495 CVE-2017-7502
CVE-2017-7526 CVE-2017-7541 CVE-2017-7585 CVE-2017-7586 CVE-2017-7616
CVE-2017-7741 CVE-2017-7742 CVE-2017-7771 CVE-2017-7772 CVE-2017-7773
CVE-2017-7774 CVE-2017-7775 CVE-2017-7776 CVE-2017-7777 CVE-2017-7778
CVE-2017-7805 CVE-2017-7867 CVE-2017-7868 CVE-2017-7869 CVE-2017-7895
CVE-2017-8105 CVE-2017-8106 CVE-2017-8287 CVE-2017-8361 CVE-2017-8362
CVE-2017-8363 CVE-2017-8365 CVE-2017-8890 CVE-2017-8924 CVE-2017-8925
CVE-2017-9047 CVE-2017-9048 CVE-2017-9049 CVE-2017-9050 CVE-2017-9074
CVE-2017-9075 CVE-2017-9076 CVE-2017-9077 CVE-2017-9233 CVE-2017-9242
CVE-2017-9287 CVE-2017-9605 CVE-2017-10053 CVE-2017-10067 CVE-2017-10074
CVE-2017-10081 CVE-2017-10087 CVE-2017-10089 CVE-2017-10090
CVE-2017-10096 CVE-2017-10101 CVE-2017-10102 CVE-2017-10107
CVE-2017-10108 CVE-2017-10109 CVE-2017-10110 CVE-2017-10115
CVE-2017-10116 CVE-2017-10118 CVE-2017-10135 CVE-2017-10140
CVE-2017-10176 CVE-2017-10193 CVE-2017-10198 CVE-2017-10243
CVE-2017-10268 CVE-2017-10378 CVE-2017-10379 CVE-2017-10384
CVE-2017-10661 CVE-2017-10662 CVE-2017-10663 CVE-2017-10911
CVE-2017-11103 CVE-2017-11108 CVE-2017-11176 CVE-2017-11541
CVE-2017-11542 CVE-2017-11543 CVE-2017-12837 CVE-2017-12883
CVE-2017-12893 CVE-2017-12894 CVE-2017-12895 CVE-2017-12896
CVE-2017-12897 CVE-2017-12898 CVE-2017-12899 CVE-2017-12900
CVE-2017-12901 CVE-2017-12902 CVE-2017-12985 CVE-2017-12986
CVE-2017-12987 CVE-2017-12988 CVE-2017-12989 CVE-2017-12990
CVE-2017-12991 CVE-2017-12992 CVE-2017-12993 CVE-2017-12994
CVE-2017-12995 CVE-2017-12996 CVE-2017-12997 CVE-2017-12998
CVE-2017-12999 CVE-2017-13000 CVE-2017-13001 CVE-2017-13002
CVE-2017-13003 CVE-2017-13004 CVE-2017-13005 CVE-2017-13006

CVE-2017-13007 CVE-2017-13008 CVE-2017-13009 CVE-2017-13010
CVE-2017-13011 CVE-2017-13012 CVE-2017-13013 CVE-2017-13014
CVE-2017-13015 CVE-2017-13016 CVE-2017-13017 CVE-2017-13018
CVE-2017-13019 CVE-2017-13020 CVE-2017-13021 CVE-2017-13022
CVE-2017-13023 CVE-2017-13024 CVE-2017-13025 CVE-2017-13026
CVE-2017-13027 CVE-2017-13028 CVE-2017-13029 CVE-2017-13030
CVE-2017-13031 CVE-2017-13032 CVE-2017-13033 CVE-2017-13034
CVE-2017-13035 CVE-2017-13036 CVE-2017-13037 CVE-2017-13038
CVE-2017-13039 CVE-2017-13040 CVE-2017-13041 CVE-2017-13042
CVE-2017-13043 CVE-2017-13044 CVE-2017-13045 CVE-2017-13046
CVE-2017-13047 CVE-2017-13048 CVE-2017-13049 CVE-2017-13050
CVE-2017-13051 CVE-2017-13052 CVE-2017-13053 CVE-2017-13054
CVE-2017-13055 CVE-2017-13089 CVE-2017-13090 CVE-2017-13687
CVE-2017-13688 CVE-2017-13689 CVE-2017-13690 CVE-2017-13725
CVE-2017-14062 CVE-2017-14106 CVE-2017-14340 CVE-2017-14952
CVE-2017-1000100 CVE-2017-1000101 CVE-2017-1000111 CVE-2017-1000112
CVE-2017-1000158 CVE-2017-1000251 CVE-2017-1000254 CVE-2017-1000257
CVE-2017-1000363 CVE-2017-1000364 CVE-2017-1000365 CVE-2017-1000366
CVE-2017-1000367 CVE-2017-1000376 CVE-2017-1000379 CVE-2017-1000380

Appliance Hardware

- **VTM-34900** Fixed an issue where jetNexus ETM E5 appliances could have network ports named in a non-deterministic order.

Virtual Appliance

- **VTM-33584** Fixed an issue where the Networking page of the Admin UI did not allow an IP address of a bond interface to be deleted if the interface had a VLAN child and the IP address was the first one to be added to the interface.
- **VTM-32973** Fixed an issue whereby a VLAN tagged IP address on a bonded interface on an appliance would not be raised until the appliance was rebooted.

Cloud Platforms

- **VTM-33751** Fixed an issue where the 'nameip' setting would be disabled after upgrading a Google Compute Engine Virtual Appliance.

7) WEB APPLICATION FIREWALL

- The traffic manager will install version 4.9-43062 of the Pulse Secure Virtual Web Application Firewall.
- Fixed an Updater UI issue where it was reporting an upgrade failure even after successful upgrade

- Enhanced ValidHTTPMethodHandler to allow CalDAV methods.
- Added support for customizable subject and filename for report emails.
- Added null byte detection to baseline protection handler.
- Added support for custom client IP HTTP header.
- Fixed syntax error in start script for SmartOS.
- Fixed an issue that could occasionally cause an error while loading the event log.
- Updated zlib to zlib-1.2.11.
- **VTM-31898** Running the z-reset-to-factory-defaults script on an appliance will no longer remove the /logs/stingrayafm directory used by the Brocade vWAF, the previous behavior could cause upgrades to fail.
- **VTM-19299**, **VTM-32184**, **VTM-23364**, **VTM-22224**, **VTM-22207**, **SR24140**, **SR30724**, **SR29025**, **SR29004** The maximum number of application firewall decider processes that can be used has been increased from 8 to 64.

8) KNOWN ISSUES IN 9.9R3

Upgrading Virtual Appliances from 9.9, 9.9r1 or 9.9r2

- When upgrading to 9.9r3 on a Stingray Traffic Manager appliance, the Admin UI will restart while the upgrade is still in progress. Users should log into the Admin UI and reboot the appliance when prompted on the home screen to complete the upgrade.

9) CONTACTING SUPPORT

Visit the Pulse Secure Web site to download software updates and documentation, browse our library of Knowledge Center articles and manage your account.

To request support, go to https://www.pulsesecure.net/support/