PULSE SECURE PRODUCT RELEASE NOTES

PRODUCT: BROCADE VIRTUAL TRAFFIC MANAGER

RELEASE DATE: 30TH SEPTEMBER, 2019

VERSION: 17.2R3

CONTENTS

1) ABOUT THIS RELEASE

The Brocade Virtual Traffic Manager 17.2r3 is a maintenance release of the Brocade Virtual Traffic Manager product family, containing a number of performance and functionality enhancements and bug fixes. Customers are recommended to upgrade to this version to take advantage of the changes.

2) PLATFORM AVAILABILITY

- Linux x86_64: Kernel 2.6.32 - 4.4, glibc 2.12+

- Virtual Appliances:
  - VMware vSphere 6.0, 6.5;
  - XenServer 7.1;
  - Microsoft Hyper-V Server 2016;
  - Microsoft Hyper-V under Windows Server 2016;
  - QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 16.04);
- Amazon EC2 - as a virtual appliance or native software install
- Microsoft Azure - as a virtual appliance
- Google Compute Engine - as a virtual appliance or native software install
- Bare Metal Server - for information on qualified servers, please see the Pulse Secure vTM Hardware Compatibility List at:

  https://www.pulsesecure.net/techpubs

3) RESOURCE REQUIREMENTS

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

Appliances intended for use with Data Plane Acceleration mode should be allocated a minimum of 3GB of RAM, and have a minimum of 2 cores. An additional 1GB of RAM is needed for each additional core for application data processing.

4) UPGRADING TO 17.2R3

17.2r3 can be installed directly using any supported installation mechanism.

Traffic manager software installations can be upgraded directly to 17.2r3 using any supported upgrade mechanism.

Traffic manager instances (appliance or cloud) running release 17.2 can be upgraded directly to 17.2r3 using any supported upgrade mechanism.

Traffic manager instances (appliance or cloud) running versions prior to 17.2 must first be upgraded to 17.2.

5) CHANGES IN 17.2R3

Installation and Upgrading

- **VTM-40471** Fixed an issue where installing a hotfix via the command line did not record it in the list of applied hotfixes.

Configuration

- **VTM-41447** Fixed a value encoding issue in the "Backup my configuration" Wizard.
- **VTM-39010** Fixed a value encoding issue in the backup restore wizard in the Admin UI.
- **VTM-27677** Fixed an issue where location names containing HTML tags were rendered incorrectly on the Backup Comparisons page of the Admin UI.

Performance

- **VTM-36154** The output of the 'mtrace' tool has been extended with additional metadata.

Authentication

- **VTM-41451** Updated the OpenLDAP library used by the traffic manager to version 2.4.47, addressing CVE-2015-6908.
- **VTM-36477** The MIT Kerberos libraries used by the traffic manager have been updated to version 1.14.6. This includes a fix for the security issue reported in CVE-2014-9423.

Administration Server

- **VTM-42283** The version of the expat XML parser library used in the Administration Server has been increased to 2.2.8, addressing CVE-2019-15903.
- **VTM-12631, VTM-41647, VTM-35880, SR16452** The Administration Server no longer returns a "Server" header in its HTTP responses.
- **VTM-41675** The version of the expat XML parser library used in the Administration Server has been increased to 2.2.7, addressing CVE-2018-20843.
- **VTM-41577, VTM-41578** Fixed a value encoding issue on the Historical Activity page in the Admin UI.
- **VTM-41387, VTM-39011** Fixed a value encoding issue on the Current Activity page in the Admin UI.
- **VTM-41375** Fixed a value encoding issue for dropdown boxes in the Admin UI.

- **VTM-40220** The upstream fix for CVE-2018-18311 was applied to the version of Perl included in the product.
- **VTM-15293, SR19322** Fixed an issue where restarting the Admin server could cause high CPU usage when multiple browsers were connected to the Admin UI.
- **VTM-36341** Added additional HTTP Cache-Control options to dynamically generated Admin UI pages to ensure they are not incorrectly cached or stored.
- **VTM-39009** Fixed a value encoding issue in Wizard pages in the Admin UI; the wizards are used to guide authorized users through various configuration tasks.
- **VTM-38803** Fixed an issue where files in the Admin Server docroot were unnecessarily visible via directory listings to users who had logged into the Admin UI.
- **VTM-38800** All Admin UI cookies are now marked as "secure" as they are only used by resources served over HTTPS connections.
- **VTM-38801, VTM-29994** Fixed an issue where a 500 Internal Server error response would be returned if an unknown wizard section was visited; now a 404 response will be produced.
- **VTM-23453, VTM-19065, SR30839, SR23813** Auto-completion of the password field on the login page of the Admin UI has been disabled to improve security.
- **VTM-36342** Added Content-Security-Policy HTTP headers in responses from the traffic manager's Admin UI. This improves security for administrators using user agents that support this standard. Note that the vWAF UI pages do not currently provide Content-Security-Policy headers.
- **VTM-19083, SR23836** Added X-Frame-Options, X-Content-Type-Options and X-XSS-Protection HTTP headers in responses from the Admin UI to enable the additional security protection measures in user agents where they are supported.

REST API

- **VTM-37368** The REST API has been modified to correctly generate the schemas for dynamic type resources.
- **VTM-40020** Fixed an issue where a REST API endpoint with simultaneous writers and readers could occasionally stop responding to new requests.
- **VTM-35351** Fixed an issue where GET of a REST resource in the status tree (/api/tm/VERSION/status/) could fail when the traffic manager configuration was very large.

Zeusbench

- **VTM-29855** Fixed an issue related to zeusbench's '-w' (warmup) option. With that option in use, the final summary of the benchmark run included connections made during the warmup period in the count for total connections made. Furthermore, when used in conjunction with the verbose option, columns 'Reqs', 'Resps', 'Established' and 'Connecting' in the verbose output could show incorrect values.
- **VTM-35444** Fixed an issue where running Zeusbench when specifying both -c 0 and --http2 caused an assertion failure.
- **VTM-35441** Updated the Zeusbench performance benchmarking tool to support TCP connection concurrency step-up with HTTP/2 requests.
- **VTM-35437, VTM-36151** Fixed an issue where running zeusbench with --http2 and -v incorrectly showed the number of HTTP/2 streams in the "Sockets" and "Connecting" columns. It now correctly shows the number of TCP connections.

SNMP

- **VTM-31957** Fixed an issue where the counters "Bandwidth", "Bandwidth per Node", "Bandwidth per Pool", and "Bandwidth per Virtual Server" were not available to select from the values to monitor when changing the data to plot on 'Current Activity' page on the Admin UI.

TrafficScript

- **VTM-41764** The libxslt library incorporated in the traffic manager has been updated to version 1.1.33 and had fixes for CVE-2019-13117 and CVE-2019-13118 applied.
- **VTM-40987** The Perl Compatible Regular Expression library (PCRE) has been updated to version 10.32, addressing CVE-2017-8399.

Connection Queueing

- **VTM-41170** Fixed an issue that could have prevented an error page being sent to a client if their request was timed out when waiting in a queue.

Connection Processing

- **VTM-42306** Limited the number of HTTP/2 frames queued per connection to 10,000 when the TCP buffers for that connection are full. This is significantly more than is expected that an RFC 7540 protocol-following HTTP/2 client would generate. This mitigates against excessive memory increases caused by superfluous HTTP/2 frame floods, and protects against the following denial-of-service attacks: CVE-2019-9511, CVE-2019-9512, CVE-2019-9514 and CVE-2019-9515.
- **VTM-40135** Fixed incorrect text in HTTP/2 request tracing, where previously the traffic manager closing the stream to the client was logged as "Client closed HTTP/2 stream" it is now correctly logged as "Traffic Manager closed HTTP/2 stream".

- **VTM-39145** The traffic manager's built-in DNS server no longer rejects client DNS requests with the RA (recursion available) flag set to true.
- **VTM-38859** Fixed an issue where a traffic manager child process could stop processing traffic after receiving an HTTP/2 SETTINGS frame, with the corresponding child process automatically being restarted after a short period to recover from the error state.
- **VTM-38729, VTM-40803** Fixed an issue that could occur when an HTTP/2 stream is closed.
- **VTM-38141** Upload speed over high-latency HTTP/2 connections has been significantly improved. Previously, if the http2!stream_window_size setting was increased to cater for high-latency connections, the connection window was not correspondingly resized and continued to limit the upload speed. The connection window is now sized appropriately for the streams it handles.

Fault Tolerance

- **VTM-41613** Fixed a value encoding issue in the "Join a cluster" Wizard.
- **VTM-29802, VTM-38731** Fixed an issue where the Diagnose page would report the version of an uncontactable traffic manager to be "2.0", and display an error that not all cluster members are using the same traffic manager version.

IP Transparency

- **VTM-25118, VTM-26241, SR34508** Fixed an issue where the traffic manager reported not being able to initialize the ip6tables mangle table when running on a Linux host without IPv6 support.

Health Monitoring

- **VTM-18479, SR23104** Fixed an issue where back-end nodes that are marked as failed by a health monitor, then are marked as disabled or deleted from the pool by the administrator when in the failed state, and finally recover and are re-enabled or re-added to the pool by the administrator, do not receive traffic.

Global Load Balancing

- **VTM-42055** Updated GeoIP database to 2019-08-06.
- **VTM-41530** Fixed an issue in GLB clustered setups where the recovery of a service would not cause its Service IP address to be returned to clients for which it was the closest. The clients would instead keep getting the IP address of the service that was the closest working before the optimal one recovered.
- **VTM-39711** Fixed an issue where a GLB service sometimes returned the IP addresses of "Draining" locations.

Map

- **VTM-39012** Fixed a value encoding issue in the 'Activity > Map' page of the Admin UI.

Licensing

- **VTM-40304** Fixed an issue where an error condition for a FLA license key would continue to be reported if a child zeus.zxtm process exited and was restarted even after the error condition had been cleared.

SSL/TLS and Cryptography

- **VTM-39995** The library modified from OpenSSL that is used by the traffic manager has been upgraded to version 1.0.2s, addressing CVE-2018-0732, CVE-2018-0737, CVE-2018-0734 and CVE-2018-5407. This library is used to provide cryptographic primitives like RSA or AES.

FIPS

- **VTM-37541** The SSL/TLS ciphers "SSL_RSA_WITH_3DES_EDE_CBC_SHA" and "SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA" are no longer available in FIPS mode to comply the with the NIST regulations in SP 800 67 revision 2.

Logging

- **VTM-40238** Fixed a value encoding issue in the alerting Event Types edit page in the Admin UI.
- **VTM-30456** The format of remote syslog messages sent by the traffic manager's request logging and event log components has been updated to follow the specification defined in RFC 5424. Accordingly, syslog messages now contain hostname and timestamp information, and the default value for the maximum length of a remote syslog message has changed from 1024 bytes to 2048 bytes.

Web Accelerator

- **VTM-40739** Web Accelerator has been updated to use libjpeg version 9c

Pool Autoscaling

- **VTM-41784** Fixed an issue where autoscaling TLS connections to VMware vSphere would sometimes fail, resulting in autoscaling being disabled.
- **VTM-40804** Fixed an issue which could cause the autoscaler process to restart if a pool was configured to use both autoscaling and DNS-derived autoscaling.

Internals

- **VTM-40528** Fixed an issue where TrafficScript code that accesses array elements by the direct use of a function call could, in some specific circumstances, cause an ASSERT failure.
- **VTM-38351** Fixed an issue where the JSON parser used by the traffic manager in, for example, TrafficScript or the Service Discovery feature, could exhaust the stack while parsing a deeply nested JSON data structure leading to a crash. The traffic manager will now reject such JSON data structures with an error message.

Appliance OS

- **VTM-42335** Updated appliance kernel to 4.4.0-164.192 and updated packages installed on the appliance.These updates include changes addressing:

  CVE-2011-5325 CVE-2015-9261 CVE-2015-9262 CVE-2015-9383 CVE-2016-2147
  CVE-2016-2148 CVE-2016-3119 CVE-2016-3120 CVE-2016-3189 CVE-2016-6153
  CVE-2016-7076 CVE-2016-7942 CVE-2016-7943 CVE-2016-9318 CVE-2016-10087
  CVE-2016-10165 CVE-2016-10254 CVE-2016-10255 CVE-2016-10708
  CVE-2016-10745 CVE-2017-2518 CVE-2017-2519 CVE-2017-2520 CVE-2017-5953
  CVE-2017-6519 CVE-2017-6892 CVE-2017-7526 CVE-2017-7607 CVE-2017-7608
  CVE-2017-7609 CVE-2017-7610 CVE-2017-7611 CVE-2017-7612 CVE-2017-7613
  CVE-2017-10989 CVE-2017-11368 CVE-2017-11462 CVE-2017-12447
  CVE-2017-13166 CVE-2017-13168 CVE-2017-13305 CVE-2017-13685
  CVE-2017-13695 CVE-2017-14245 CVE-2017-14246 CVE-2017-14634
  CVE-2017-15873 CVE-2017-16538 CVE-2017-16544 CVE-2017-16942
  CVE-2017-17456 CVE-2017-17457 CVE-2017-17975 CVE-2017-18174
  CVE-2017-18193 CVE-2017-18216 CVE-2017-18222 CVE-2017-18241
  CVE-2017-18248 CVE-2017-18249 CVE-2017-18255 CVE-2017-18257
  CVE-2017-18258 CVE-2017-18344 CVE-2017-1000368 CVE-2018-0494
  CVE-2018-0495 CVE-2018-0732 CVE-2018-0734 CVE-2018-0737 CVE-2018-1060
  CVE-2018-1061 CVE-2018-1065 CVE-2018-1068 CVE-2018-1087 CVE-2018-1092
  CVE-2018-1093 CVE-2018-1120 CVE-2018-1122 CVE-2018-1123 CVE-2018-1124
  CVE-2018-1125 CVE-2018-1126 CVE-2018-1130 CVE-2018-1152 CVE-2018-2783
  CVE-2018-2790 CVE-2018-2794 CVE-2018-2795 CVE-2018-2796 CVE-2018-2797
  CVE-2018-2798 CVE-2018-2799 CVE-2018-2800 CVE-2018-2814 CVE-2018-2815
  CVE-2018-2952 CVE-2018-3136 CVE-2018-3139 CVE-2018-3149 CVE-2018-3169
  CVE-2018-3180 CVE-2018-3183 CVE-2018-3214 CVE-2018-3620 CVE-2018-3639
  CVE-2018-3646 CVE-2018-3665 CVE-2018-4180 CVE-2018-4181 CVE-2018-4700
  CVE-2018-5383 CVE-2018-5390 CVE-2018-5391 CVE-2018-5407 CVE-2018-5729
  CVE-2018-5730 CVE-2018-5740 CVE-2018-5743 CVE-2018-5745 CVE-2018-5750
  CVE-2018-5803 CVE-2018-5814 CVE-2018-5873 CVE-2018-6553 CVE-2018-6554
  CVE-2018-6555 CVE-2018-6954 CVE-2018-7183 CVE-2018-7185 CVE-2018-7456
  CVE-2018-7480 CVE-2018-7566 CVE-2018-7740 CVE-2018-7755 CVE-2018-7757
  CVE-2018-7995 CVE-2018-8087 CVE-2018-8781 CVE-2018-8822 CVE-2018-8897
  CVE-2018-8905 CVE-2018-9363 CVE-2018-9385 CVE-2018-9415 CVE-2018-9422
  CVE-2018-9516 CVE-2018-9517 CVE-2018-9518 CVE-2018-10021 CVE-2018-10087

CVE-2018-10124 CVE-2018-10360 CVE-2018-10779 CVE-2018-10844
CVE-2018-10845 CVE-2018-10846 CVE-2018-10853 CVE-2018-10876
CVE-2018-10877 CVE-2018-10878 CVE-2018-10879 CVE-2018-10880
CVE-2018-10881 CVE-2018-10882 CVE-2018-10883 CVE-2018-10902
CVE-2018-10938 CVE-2018-10940 CVE-2018-10963 CVE-2018-11490
CVE-2018-12015 CVE-2018-12020 CVE-2018-12126 CVE-2018-12127
CVE-2018-12130 CVE-2018-12233 CVE-2018-12384 CVE-2018-12404
CVE-2018-12896 CVE-2018-12900 CVE-2018-13053 CVE-2018-13094
CVE-2018-13096 CVE-2018-13097 CVE-2018-13099 CVE-2018-13100
CVE-2018-13139 CVE-2018-13405 CVE-2018-13406 CVE-2018-14404
CVE-2018-14567 CVE-2018-14598 CVE-2018-14599 CVE-2018-14600
CVE-2018-14609 CVE-2018-14610 CVE-2018-14611 CVE-2018-14612
CVE-2018-14613 CVE-2018-14614 CVE-2018-14616 CVE-2018-14617
CVE-2018-14618 CVE-2018-14633 CVE-2018-14647 CVE-2018-14679
CVE-2018-14680 CVE-2018-14681 CVE-2018-14682 CVE-2018-14734
CVE-2018-15473 CVE-2018-15572 CVE-2018-15594 CVE-2018-15686
CVE-2018-15687 CVE-2018-15688 CVE-2018-16062 CVE-2018-16276
CVE-2018-16402 CVE-2018-16403 CVE-2018-16428 CVE-2018-16429
CVE-2018-16435 CVE-2018-16658 CVE-2018-16839 CVE-2018-16842
CVE-2018-16862 CVE-2018-16864 CVE-2018-16865 CVE-2018-16866
CVE-2018-16884 CVE-2018-16890 CVE-2018-17000 CVE-2018-17100
CVE-2018-17101 CVE-2018-17182 CVE-2018-17972 CVE-2018-18021
CVE-2018-18065 CVE-2018-18074 CVE-2018-18310 CVE-2018-18311
CVE-2018-18312 CVE-2018-18313 CVE-2018-18314 CVE-2018-18508
CVE-2018-18520 CVE-2018-18521 CVE-2018-18557 CVE-2018-18584
CVE-2018-18585 CVE-2018-18661 CVE-2018-18690 CVE-2018-18710
CVE-2018-18751 CVE-2018-19210 CVE-2018-19407 CVE-2018-19432
CVE-2018-19661 CVE-2018-19662 CVE-2018-19758 CVE-2018-19824
CVE-2018-19985 CVE-2018-20060 CVE-2018-20169 CVE-2018-20346
CVE-2018-20406 CVE-2018-20506 CVE-2018-20511 CVE-2018-20679
CVE-2018-20685 CVE-2018-20836 CVE-2018-20843 CVE-2018-20852
CVE-2018-20856 CVE-2018-1000004 CVE-2018-1000030 CVE-2018-1000199
CVE-2018-1000204 CVE-2018-1000301 CVE-2018-1000517 CVE-2018-1000802
CVE-2018-1000845 CVE-2019-0804 CVE-2019-0816 CVE-2019-1125 CVE-2019-1559
CVE-2019-2024 CVE-2019-2054 CVE-2019-2101 CVE-2019-2422 CVE-2019-2602
CVE-2019-2684 CVE-2019-2697 CVE-2019-2698 CVE-2019-2745 CVE-2019-2762
CVE-2019-2769 CVE-2019-2786 CVE-2019-2816 CVE-2019-2842 CVE-2019-3459
CVE-2019-3460 CVE-2019-3462 CVE-2019-3701 CVE-2019-3819 CVE-2019-3822
CVE-2019-3823 CVE-2019-3832 CVE-2019-3842 CVE-2019-3846 CVE-2019-3874
CVE-2019-3882 CVE-2019-3900 CVE-2019-5010 CVE-2019-5436 CVE-2019-5482
CVE-2019-5747 CVE-2019-5953 CVE-2019-6109 CVE-2019-6111 CVE-2019-6128
CVE-2019-6133 CVE-2019-6454 CVE-2019-6465 CVE-2019-6974 CVE-2019-7149
CVE-2019-7150 CVE-2019-7221 CVE-2019-7222 CVE-2019-7317 CVE-2019-7663
CVE-2019-7665 CVE-2019-8457 CVE-2019-8675 CVE-2019-8696 CVE-2019-8905
CVE-2019-8907 CVE-2019-9213 CVE-2019-9503 CVE-2019-9636 CVE-2019-9740
CVE-2019-9893 CVE-2019-9924 CVE-2019-9936 CVE-2019-9937 CVE-2019-9947

CVE-2019-9948 CVE-2019-10126 CVE-2019-10142 CVE-2019-10160 CVE-2019-10638 CVE-2019-10639 CVE-2019-10906 CVE-2019-11091 CVE-2019-11190 CVE-2019-11191 CVE-2019-11236 CVE-2019-11477 CVE-2019-11478 CVE-2019-11479 CVE-2019-11599 CVE-2019-11719 CVE-2019-11729 CVE-2019-11810 CVE-2019-11815 CVE-2019-11833 CVE-2019-11884 CVE-2019-12450 CVE-2019-12614 CVE-2019-12735 CVE-2019-12749 CVE-2019-12818 CVE-2019-12819 CVE-2019-12900 CVE-2019-13012 CVE-2019-13057 CVE-2019-13272 CVE-2019-13565 CVE-2019-13648 CVE-2019-14283 CVE-2019-14284 CVE-2019-14835 CVE-2019-15133 CVE-2019-15903 CVE-2019-1010305

- **VTM-37057, VTM-38971** Fixed an issue where importing a configuration backup made on a pre-17.2 traffic manager would not have restored traffic manager-specific settings. When such a configuration backup import is carried out the interface names will not be changed, and configuration may need to be adjusted manually.
- **VTM-41745** Fixed an issue in the timezone field of UI wizards so that invalid timezones are no longer accepted
- **VTM-41786** Wizards displayed by the Administration UI now apply their validation of user-supplied data more consistently
- **VTM-38760** The VMware appliance now contains the VMware balloon kernel module.
- **VTM-18677, SR23373** It is now possible to set the interface MTU on a traffic manager appliance on Hyper-V.
- **VTM-35587, VTM-35586, VTM-34358** Fixed an issue where an appliance upgrade would not delete the files related to the kernel being replaced from the boot partition. After a number of upgrades, this could leave insufficient space in the boot partition, causing subsequent upgrade attempts to fail.
- **VTM-40628** Fixed an issue which made the Traffic IP Groups page of the Admin UI inaccessible if Multi-Site Manager was enabled.
- **VTM-38861** Fixed an issue where virtual Traffic Manager Hardware Appliances printed "Unable to get the health status of the hardware" for non-hardware cluster peers on the Traffic Managers admin UI page.
- **VTM-37221** Fixed an issue on appliances where enabling 'appliance!ipv4_forwarding' would load the nf_conntrack module which could cause traffic to be dropped.

Virtual Appliance

- **VTM-39411** Fixed an issue where the code disabling receive and segmentation offload on appliance NICs did not run.

- **VTM-38768** Fixed issues in appliance log partition monitoring, where the traffic manager failed to generate "logdiskoverload" and "logdiskfull" events when the "/logs" partition reached thresholds of 85% or 95% full, respectively. These events are now generated correctly as soon as a new threshold is reached, and are repeated daily while that condition persists. Recovery occurs the next day if use has dropped only slightly below the threshold, or immediately if use drops to at least 5% below the threshold. Upon recovery, the traffic manager reports the new condition: either "logdiskoverload" (if recovered to between 85% and 95%), or with a new event type "logdiskrecovered" (if recovered to below 85%).

Cloud Platforms

- **VTM-42167** Traffic managers running on Amazon EC2 will no longer accept the Access Key and Secret Access Key method of authentication with AWS services. In order to use Traffic IP Groups or Pool Node Autoscaling an IAM Role must be assigned to the EC2 instance. This change applies to vTM AMIs deployed through the AWS Marketplace and vTM software installed on Linux EC2 instances. Refer to the vTM Cloud Getting Started Guide for the policies an IAM Role requires.
- **VTM-42109** Fixed an issue that caused traffic managers to fail to authenticate with the Azure Key Vault service, following a change to its behavior in August 2019.
- **VTM-36298** Fixed an issue where it was not possible to cluster GCE and AWS appliances.
- **VTM-39408** Fixed a memory leak in traffic managers running on Google Compute Engine.
- **VTM-37438** Fixed an issue where an EC2 instance would ignore user data specifying a certificate to identify a Services Director instance for licensing self-registration.

6) WEB APPLICATION FIREWALL

The traffic manager will install version 4.9-43062 of the Pulse Secure Virtual Web Application Firewall.

7) KNOWN ISSUES IN 17.2R3

There are no additional known issues in 17.2r3. See the section on Known Issues in 17.2.

8) 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/