PULSE SECURE PRODUCT RELEASE NOTES

PRODUCT: PULSE SECURE VIRTUAL TRAFFIC MANAGER

RELEASE DATE: 30TH SEPTEMBER, 2019

VERSION: 18.2R1

CONTENTS

1) ABOUT THIS RELEASE

The Pulse Secure Virtual Traffic Manager 18.2r1 is a maintenance release of the Pulse Secure 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

Virtual Traffic Manager software

- Linux x86_64: Kernel 2.6.32 - 4.15, glibc 2.12+
  For Route Health Injection: ncurses 5 (libncurses.so.5, libtinfo.so.5)

Virtual Traffic Manager containers

- Docker: 1.13.0 or later recommended

Virtual Traffic Manager virtual appliances

- VMware vSphere 6.0, 6.5
- XenServer 7.1
- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V under Windows 2016
- QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 16.04)

Virtual Traffic Manager cloud platforms

- 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

Virtual Traffic Manager physical appliances

- Bare Metal Server - for information on qualified servers, 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.

4) UPGRADING TO 18.2R1

18.2r1 can be installed directly using any supported installation mechanism. Traffic manager software installations can be upgraded directly to 18.2r1 using any supported upgrade mechanism, except those running traffic manager version 17.2 which must be upgraded to some other version (for example 17.2r3 or 18.2) before upgrading.

Traffic manager instances (appliance or cloud) running release 18.2 can be upgraded directly to 18.2r1 using any supported upgrade mechanism.

Traffic manager instances (appliance or cloud) running versions prior to 18.2 must first be upgraded to 18.2.

5) CHANGES IN 18.2R1

Installation and Upgrading

- **VTM-37935**, **VTM-38535** Fixed an issue when applying a hotfix to a cluster which caused it to be recorded on the traffic manager where the upgrade was initiated rather than the cluster members where it was applied.
- **VTM-40471** Fixed an issue where installing a hotfix via the command line did not record it in the list of applied hotfixes.
- **VTM-38544**, **VTM-37767** Fixed an issue where applying a hotfix with the upgrade-cluster tool would not restart the remote traffic managers automatically to apply the hotfix changes.

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.

Authentication

- **VTM-41451** Updated the OpenLDAP library used by the traffic manager to version 2.4.47, addressing CVE-2015-6908.

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.

REST API

- **VTM-37368** The REST API has been modified to correctly generate the schemas for dynamic type resources.
- **VTM-41159** Fixed an issue where requesting metadata for SSL certificates caused the REST API to crash
- **VTM-40020** Fixed an issue where a REST API endpoint with simultaneous writers and readers could occasionally stop responding to new requests.

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.
- **VTM-40554** Fixed an issue that, when the traffic manager is receiving a POST request with a large body and a TrafficScript rule aborts due to a usage error, results in connections being dropped or denied.

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.

Fault Tolerance

- **VTM-41613** Fixed a value encoding issue in the "Join a cluster" Wizard.
- **VTM-40372** Fixed an issue where the traffic manager would stall when sending data on an SSL connection, if the socket buffer became full while writing out the last bytes of a response. In particular, this impacted control plane status messages when the traffic manager configuration was large (more than ~50 configuration objects).

IP Transparency

- **VTM-40280** Fixed an issue that prevented the virtual server transparent proxying feature settings from being displayed in the Admin UI.

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-41999** 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.

Service Discovery

- **VTM-40033** Fixed an issue that prevented the 'interval_override' parameter in a Service Discovery plugin's output from taking effect.
- **VTM-39742** Fixed an issue where the nodes list of a Service Discovery pool could be erased on a traffic manager which was restarted after the nodes list was populated.

- **VTM-39581** Fixed an issue where quotes in the plugin arguments specified in Service Discovery pools would be incorrectly passed to the plugin. The traffic manager now emulates a shell and treats text within a pair of quotes as a single argument, while removing the quote characters.
- **VTM-38197** Fixed an issue where using a malformed Service Discovery plugin would cause an error to be printed to the event log every 10 seconds instead of once.

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-41220** Fixed an issue where the per-pool configuration settings for the policy around caching SSL client sessions or session tickets for pool nodes were not correctly respected until the traffic manager was restarted.
- **VTM-39996** 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.

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
- **VTM-40454** Fixed an issue that caused Web Accelerator to return pages with HTTP Date and Expires headers that had incorrect timestamps, reducing the effectiveness of downstream caching.

Pool Autoscaling

- **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.

Telemetry

- **VTM-17840, SR22270** The traffic manager's telemetry system has been updated to report anonymized data in the event of certain traffic manager processes failing.

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-40771** Changes to the mtrace utility address the following vulnerabilities: CVE-2016-10254 and CVE-2016-10255

6) VIRTUAL TRAFFIC MANAGER APPLIANCE

Appliance OS

- **VTM-42343** Updated the appliance kernel to 4.15.0-64.73, and updated packages installed on the appliance. These updates include changes addressing:

  CVE-2016-3977 CVE-2016-9318 CVE-2017-6519 CVE-2017-13168 CVE-2017-13695 CVE-2017-14245 CVE-2017-14246 CVE-2017-14634 CVE-2017-16932 CVE-2017-17456 CVE-2017-17457 CVE-2017-18258 CVE-2018-0495 CVE-2018-0501 CVE-2018-0734 CVE-2018-0735 CVE-2018-1093 CVE-2018-1108 CVE-2018-1118 CVE-2018-1120 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-2018-3646 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-2018-5744 CVE-2018-5745 CVE-2018-5814 CVE-2018-6554 CVE-2018-6555 CVE-2018-6557 CVE-2018-6559 CVE-2018-6954 CVE-2018-8905 CVE-2018-9363 CVE-2018-9385 CVE-2018-9415 CVE-2018-9516 CVE-2018-9518 CVE-2018-10323 CVE-2018-10779 CVE-2018-10840 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-2018-10903 CVE-2018-10963 CVE-2018-11412 CVE-2018-11490 CVE-2018-11506 CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2018-12232 CVE-2018-12233 CVE-2018-12384 CVE-2018-12404 CVE-2018-12896 CVE-2018-12900 CVE-2018-12904 CVE-2018-13053 CVE-2018-13093 CVE-2018-13094 CVE-2018-13096 CVE-2018-13097 CVE-2018-13098 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-2018-14615 CVE-2018-14616 CVE-2018-14617 CVE-2018-14618 CVE-2018-14625 CVE-2018-14633 CVE-2018-14647 CVE-2018-14678

CVE-2018-14679 CVE-2018-14680 CVE-2018-14681 CVE-2018-14682
CVE-2018-14734 CVE-2018-15120 CVE-2018-15471 CVE-2018-15473
CVE-2018-15572 CVE-2018-15594 CVE-2018-15686 CVE-2018-15687
CVE-2018-15688 CVE-2018-15853 CVE-2018-15854 CVE-2018-15855
CVE-2018-15856 CVE-2018-15857 CVE-2018-15858 CVE-2018-15859
CVE-2018-15861 CVE-2018-15862 CVE-2018-15863 CVE-2018-15864
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-2018-16871 CVE-2018-16882
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-2018-18281 CVE-2018-18310
CVE-2018-18311 CVE-2018-18312 CVE-2018-18313 CVE-2018-18314
CVE-2018-18397 CVE-2018-18445 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-2018-18955 CVE-2018-19210 CVE-2018-19407 CVE-2018-19432
CVE-2018-19661 CVE-2018-19662 CVE-2018-19758 CVE-2018-19824
CVE-2018-19854 CVE-2018-19985 CVE-2018-20060 CVE-2018-20169
CVE-2018-20346 CVE-2018-20406 CVE-2018-20483 CVE-2018-20505
CVE-2018-20506 CVE-2018-20511 CVE-2018-20679 CVE-2018-20685
CVE-2018-20784 CVE-2018-20836 CVE-2018-20843 CVE-2018-20852
CVE-2018-20856 CVE-2018-1000200 CVE-2018-1000204 CVE-2018-1000517
CVE-2018-1000802 CVE-2018-1000845 CVE-2018-1000858 CVE-2019-0136
CVE-2019-0804 CVE-2019-0816 CVE-2019-1125 CVE-2019-1559 CVE-2019-2024
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-2019-3829
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-2019-5481 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-2019-6470 CVE-2019-6471
CVE-2019-6974 CVE-2019-7149 CVE-2019-7150 CVE-2019-7221 CVE-2019-7222
CVE-2019-7308 CVE-2019-7317 CVE-2019-7663 CVE-2019-7665 CVE-2019-8457
CVE-2019-8675 CVE-2019-8696 CVE-2019-8905 CVE-2019-8906 CVE-2019-8907
CVE-2019-8912 CVE-2019-8980 CVE-2019-9213 CVE-2019-9500 CVE-2019-9503
CVE-2019-9506 CVE-2019-9636 CVE-2019-9740 CVE-2019-9893 CVE-2019-9936
CVE-2019-9937 CVE-2019-9947 CVE-2019-9948 CVE-2019-10126 CVE-2019-10160
CVE-2019-10207 CVE-2019-10638 CVE-2019-10639 CVE-2019-10906
CVE-2019-11068 CVE-2019-11085 CVE-2019-11091 CVE-2019-11191
CVE-2019-11236 CVE-2019-11324 CVE-2019-11477 CVE-2019-11478
CVE-2019-11479 CVE-2019-11487 CVE-2019-11599 CVE-2019-11719
CVE-2019-11729 CVE-2019-11810 CVE-2019-11815 CVE-2019-11833
CVE-2019-11884 CVE-2019-11922 CVE-2019-12450 CVE-2019-12614

CVE-2019-12735 CVE-2019-12749 CVE-2019-12818 CVE-2019-12819 CVE-2019-12900 CVE-2019-12984 CVE-2019-13012 CVE-2019-13057 CVE-2019-13233 CVE-2019-13272 CVE-2019-13565 CVE-2019-13631 CVE-2019-13648 CVE-2019-14283 CVE-2019-14284 CVE-2019-14763 CVE-2019-14835 CVE-2019-15030 CVE-2019-15031 CVE-2019-15090 CVE-2019-15133 CVE-2019-15211 CVE-2019-15212 CVE-2019-15214 CVE-2019-15215 CVE-2019-15216 CVE-2019-15218 CVE-2019-15220 CVE-2019-15221 CVE-2019-15292 CVE-2019-15718 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.

Appliance Hardware

- **VTM-40018** Fixed an issue where some hardware appliances were reporting "Unable to send command: Invalid argument" IPMI errors.
- **VTM-39943** Fixed an issue where changing network cards in hardware appliances could cause interfaces to be named incorrectly.

Virtual Appliance

- **VTM-38761** Fixed an issue which prevented configuration of the VMware appliance using Guest OS Customizations.
- **VTM-39411** Fixed an issue where the code disabling receive and segmentation offload on appliance NICs did not run.

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-40368** Fixed an issue where traffic manager appliances deployed on EC2 could not use AWS CloudFormation.
- **VTM-40222** Fixed an issue which caused the status applet to incorrectly report an error when the only public IP address on an instance of our AWS Marketplace AMI was an Elastic IP TIP.
- **VTM-36298** Fixed an issue where it was not possible to cluster GCE and AWS appliances.
- **VTM-39242**, **VTM-39091** Fixed an issue which sometimes caused Azure instances not to have any swap configured.
- **VTM-39475**, **VTM-39474** Fixed an issue where the names of Azure instances were not added to the Azure DNS resolver.
- **VTM-39408** Fixed a memory leak in traffic managers running on Google Compute Engine.
- **VTM-39088** Fixed an issue where an upgrade package could be incorrectly rejected due to a timeout during the package validation.

7) KNOWN ISSUES IN 18.2R1

KVM Network Interface Card renaming

- **VTM-34654** In rare circumstances a KVM host may change the PCI addresses of a virtual appliance's network cards after a reboot, resulting in the network interface labels changing. This can be fixed by removing the configuration from the non-existent card on the traffic manager 'Networking' page and re-adding it to the correct card.

Obsolete counters are missing from old REST API versions

- **VTM-38881** Obsolete counters removed from version 6.0 of the status API are missing in versions 5.X and 4.0, despite the schemata published with the product claiming they are still present.

The format of encrypted bootloader passwords has changed in version 18.2

- **VTM-38948** When upgrading from an earlier version with a bootloader password set, the bootloader will be unprotected, and a configuration error will be reported until the password is re-entered. It can be set on the Global Settings page of the Admin UI.

After VA rollback from 18.2 the rollback UI widget doesn't appear

- **VTM-38962** After rolling back from 18.2 to an earlier vTM version the rollback version selector on the Traffic Managers page of the Admin UI will not offer version 18.2 as an option. Use "$ZEUSHOME/zxtm/bin/rollback" from the command line to switch back to 18.2 instead.

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/