Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 18.2r2

Product Release	**18.2r2**
Published	**September 15, 2020**
Document Version	**1.0**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Pulse Secure Virtual Traffic Manager: Release Notes

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Release Notes

About this Release

Pulse Secure Virtual Traffic Manager 18.2r2 is a maintenance release of the Pulse Secure Virtual Traffic Manager product family, containing a number of bug fixes and security updates. Customers are recommended to upgrade to this version to take advantage of the changes.

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 Server 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

Resource Requirements

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

Upgrading to 18.2r2

18.2r2 can be installed directly using any supported installation mechanism.

Traffic Manager software installations can be upgraded directly to 18.2r2 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 18.2r2 using any supported upgrade mechanism.

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

Changes in 18.2r2

Installation and Upgrading

- **VTM-42672** Fixed a bug where the configure script would still loop if `--noloop` was provided but clustering failed.
- **VTM-42476** The script used to list installed Traffic Manager versions on appliances now uses the read-only option to mount, reducing the amount of time that operation takes.
- **VTM-42371** The Traffic Manager software installer no longer depends on the presence of the `libnsl.so` system library so that the Traffic Manager can be installed on systems whose base package set does not include `libnsl`.

Authentication

- **VTM-18659, VTM-36053, VTM-28340, VTM-23999, VTM-17657, SR23353, SR31954, SR22049** Fixed an issue where the **System > Users > Authenticators > Edit** page wasn't formatted correctly, and displayed badly in a browser. All the page elements are now aligned within the background box.

Administration Server

- **VTM-42831** Fixed an issue where the **Diagnose** and **Activity** tabs in the Traffic Manager Admin UI took excessive time to open when the Traffic Manager has many (for example, greater than 100) service discovery pools.
- **VTM-43084** Fixed an issue where the permission check needed for the addition of a rule to a virtual server or GLB service could be bypassed.
- **VTM-42432** Fixed an issue where displaying the Pools summary page in the Admin UI was slow when using Service Discovery with many pools.
- **VTM-42284** Fixes for CVE-2018-6913 and CVE-2018-18313 were applied to the version of Perl included in the product.

TrafficScript

- **VTM-43180** The Perl Compatible Regular Expression library (PCRE) has been updated to version 10.35, addressing CVE-2019-20454.
- **VTM-42419** Updated `libxslt`, which the Traffic Manager is linked against, to version 1.1.34, which fixes the following security vulnerabilities: CVE-2019-18197
- **VTM-42422** Entries in the Authenticators Catalog with `ldap!ssl` enabled and `ldap!ssl!cert` specified now include a Server Identity Check as well as verifying that the LDAP server certificate is signed by the specified certificate authority.

  Attempts by a TrafficScript rule to use such an authenticator via `auth.query()`, and that connect to a server that does not have a certificate matching its identity will fail and log a message in the event log.
- **VTM-37997** Updated `libxml2`, which the Traffic Manager is linked against, to version 2.9.9, which addresses CVE-2018-14404.

Connection Processing

- **VTM-43204** Fixed an issue where HTTP/2 requests with a single Cookie header made to a virtual server with `http2!merge_cookie_headers` enabled could result in the omission of another header field and the addition of its value to the Cookie header when a request was sent to the pool node.
- **VTM-43004** Fixed an issue where the Traffic Manager could fail a lookup of a DNS name if exactly one of IPv4 or IPv6 lookup succeeds. When a negative lookup for one was cached and not expired, but a cached positive result was expired, the negative result was returned.
- **VTM-43038, VTM-25308, SR34763** Improved HTTP/1.1 header parsing to ensure RFC 7230 section 3.2.6 is correctly followed.
- **VTM-43002** Fixed an issue which caused DNS responses in the dataplane processes to be cached only for the `dns!min_ttl` value, even when the TTL of the response is longer. This affected DNS resolution in TrafficScript rules, as well as OCSP URLs.
- **VTM-42829** Fixed an issue where a virtual server using the DNS protocol could read from heap memory after it had been freed.
- **VTM-42444** Fixed an issue where the Traffic Manager would incorrectly handle an irregular packet received by a virtual server configured to support HTTP/2, resulting in connections being dropped or denied.

Global Load Balancing

- **VTM-42979** Fixed an issue where using the `glb.service.ignoreLocation()` TrafficScript function in a GLB service rule would terminate rule processing, preventing any following TrafficScript statements from being executed.

Service Protection

- **VTM-43313** Fixed an issue that a protection class could spuriously ban an IP address permanently until either the Traffic Manager is restarted or the protection class is changed if the corresponding client sends `max_1_connections` number of HTTPS requests while the IP address is temporarily being banned due to high request rate.

- **VTM-43273** Fixed an issue that child processes could stall for excessive time if the service protection class configuration is changed while many banned HTTP connections have been responded to with error codes but the corresponding clients have not closed those TCP connections.
- **VTM-43028** Updated the behavior of the Traffic Manager when receiving an HTTP/1(.1) request with invalid whitespace between an HTTP header name and the colon, to reject the request. This behavioral change is mandated by RFC 7230.
- **VTM-43008** Fixed an issue where a malformed chunked HTTP request could cause a further request to be smuggled.

Traffic Manager Self Registration

- **VTM-42837** Fixed an issue where licensing settings (including Services Director self-registration settings) entered during the Initial Configuration Wizard were not saved.

Virtual Traffic Manager Appliance Updates

Appliance OS

- **VTM-38742** Support for `vmguestlib` has been added to the appliance image.
- **VTM-43238** Updated the appliance kernel to version 4.15.0-112.113, and updated packages installed on the appliance. These updates include changes addressing:

```
CVE-2016-9840 CVE-2016-9841 CVE-2016-9842 CVE-2016-9843 CVE-2017-16808
CVE-2018-8945 CVE-2018-9138 CVE-2018-10103 CVE-2018-10105 CVE-2018-10372
CVE-2018-10373 CVE-2018-10534 CVE-2018-10535 CVE-2018-11236 CVE-2018-11237
CVE-2018-12207 CVE-2018-12641 CVE-2018-12697 CVE-2018-12698 CVE-2018-12699
CVE-2018-12700 CVE-2018-12934 CVE-2018-13033 CVE-2018-14461 CVE-2018-14462
CVE-2018-14463 CVE-2018-14464 CVE-2018-14465 CVE-2018-14466 CVE-2018-14467
CVE-2018-14468 CVE-2018-14469 CVE-2018-14470 CVE-2018-14498 CVE-2018-14879
CVE-2018-14880 CVE-2018-14881 CVE-2018-14882 CVE-2018-16227 CVE-2018-16228
CVE-2018-16229 CVE-2018-16230 CVE-2018-16300 CVE-2018-16451 CVE-2018-16452
CVE-2018-17358 CVE-2018-17359 CVE-2018-17360 CVE-2018-17794 CVE-2018-17985
CVE-2018-18309 CVE-2018-18483 CVE-2018-18484 CVE-2018-18605 CVE-2018-18606
CVE-2018-18607 CVE-2018-18700 CVE-2018-18701 CVE-2018-19519 CVE-2018-19591
CVE-2018-19931 CVE-2018-19932 CVE-2018-20002 CVE-2018-20623 CVE-2018-20651
CVE-2018-20671 CVE-2018-20786 CVE-2018-20976 CVE-2018-21008 CVE-2018-1000876
CVE-2019-0154 CVE-2019-0155 CVE-2019-1547 CVE-2019-1549 CVE-2019-1551
CVE-2019-1563 CVE-2019-2182 CVE-2019-2201 CVE-2019-2228 CVE-2019-2894
CVE-2019-2945 CVE-2019-2949 CVE-2019-2962 CVE-2019-2964 CVE-2019-2973
CVE-2019-2975 CVE-2019-2978 CVE-2019-2981 CVE-2019-2983 CVE-2019-2987
CVE-2019-2988 CVE-2019-2989 CVE-2019-2992 CVE-2019-2999 CVE-2019-3843
CVE-2019-3844 CVE-2019-5068 CVE-2019-5094 CVE-2019-5108 CVE-2019-5188
CVE-2019-5827 CVE-2019-6477 CVE-2019-9070 CVE-2019-9071 CVE-2019-9073
CVE-2019-9074 CVE-2019-9075 CVE-2019-9077 CVE-2019-9169 CVE-2019-9674
CVE-2019-10220 CVE-2019-11135 CVE-2019-11745 CVE-2019-12290 CVE-2019-12380
CVE-2019-12972 CVE-2019-13117 CVE-2019-13118 CVE-2019-13627 CVE-2019-13734
CVE-2019-13750 CVE-2019-13751 CVE-2019-13752 CVE-2019-13753 CVE-2019-14250
CVE-2019-14287 CVE-2019-14444 CVE-2019-14615 CVE-2019-14814 CVE-2019-14815
CVE-2019-14816 CVE-2019-14821 CVE-2019-14866 CVE-2019-14895 CVE-2019-14896
CVE-2019-14897 CVE-2019-14901 CVE-2019-14973 CVE-2019-15098 CVE-2019-15099
```

CVE-2019-15117 CVE-2019-15118 CVE-2019-15165 CVE-2019-15166 CVE-2019-15167
CVE-2019-15217 CVE-2019-15291 CVE-2019-15505 CVE-2019-15538 CVE-2019-15795
CVE-2019-15796 CVE-2019-15902 CVE-2019-15918 CVE-2019-16056 CVE-2019-16089
CVE-2019-16168 CVE-2019-16229 CVE-2019-16231 CVE-2019-16232 CVE-2019-16233
CVE-2019-16234 CVE-2019-16746 CVE-2019-16935 CVE-2019-17006 CVE-2019-17007
CVE-2019-17023 CVE-2019-17052 CVE-2019-17053 CVE-2019-17054 CVE-2019-17055
CVE-2019-17056 CVE-2019-17075 CVE-2019-17133 CVE-2019-17450 CVE-2019-17451
CVE-2019-17514 CVE-2019-17546 CVE-2019-17666 CVE-2019-18197 CVE-2019-18218
CVE-2019-18224 CVE-2019-18282 CVE-2019-18348 CVE-2019-18634 CVE-2019-18660
CVE-2019-18683 CVE-2019-18786 CVE-2019-18806 CVE-2019-18809 CVE-2019-18885
CVE-2019-19036 CVE-2019-19037 CVE-2019-19039 CVE-2019-19045 CVE-2019-19046
CVE-2019-19051 CVE-2019-19052 CVE-2019-19056 CVE-2019-19057 CVE-2019-19058
CVE-2019-19060 CVE-2019-19062 CVE-2019-19063 CVE-2019-19065 CVE-2019-19066
CVE-2019-19068 CVE-2019-19071 CVE-2019-19075 CVE-2019-19078 CVE-2019-19082
CVE-2019-19083 CVE-2019-19126 CVE-2019-19227 CVE-2019-19319 CVE-2019-19332
CVE-2019-19377 CVE-2019-19447 CVE-2019-19462 CVE-2019-19523 CVE-2019-19524
CVE-2019-19525 CVE-2019-19526 CVE-2019-19527 CVE-2019-19528 CVE-2019-19529
CVE-2019-19530 CVE-2019-19531 CVE-2019-19532 CVE-2019-19533 CVE-2019-19534
CVE-2019-19535 CVE-2019-19536 CVE-2019-19537 CVE-2019-19725 CVE-2019-19767
CVE-2019-19768 CVE-2019-19807 CVE-2019-19813 CVE-2019-19816 CVE-2019-19906
CVE-2019-19922 CVE-2019-19923 CVE-2019-19925 CVE-2019-19926 CVE-2019-19956
CVE-2019-19959 CVE-2019-19965 CVE-2019-20079 CVE-2019-20096 CVE-2019-20218
CVE-2019-20367 CVE-2019-20386 CVE-2019-20636 CVE-2019-20795 CVE-2019-20806
CVE-2019-20812 CVE-2019-20907 CVE-2019-20908 CVE-2019-1010220 CVE-2020-0009
CVE-2020-0067 CVE-2020-0255 CVE-2020-1712 CVE-2020-1749 CVE-2020-1751
CVE-2020-1752 CVE-2020-2583 CVE-2020-2590 CVE-2020-2593 CVE-2020-2601
CVE-2020-2604 CVE-2020-2654 CVE-2020-2659 CVE-2020-2732 CVE-2020-2754
CVE-2020-2755 CVE-2020-2756 CVE-2020-2757 CVE-2020-2773 CVE-2020-2781
CVE-2020-2800 CVE-2020-2803 CVE-2020-2805 CVE-2020-2830 CVE-2020-3810
CVE-2020-3898 CVE-2020-5208 CVE-2020-6829 CVE-2020-7053 CVE-2020-7595
CVE-2020-8177 CVE-2020-8231 CVE-2020-8428 CVE-2020-8492 CVE-2020-8616
CVE-2020-8617 CVE-2020-8622 CVE-2020-8623 CVE-2020-8624 CVE-2020-8647
CVE-2020-8648 CVE-2020-8649 CVE-2020-8832 CVE-2020-8834 CVE-2020-8903
CVE-2020-8907 CVE-2020-8933 CVE-2020-8992 CVE-2020-9327 CVE-2020-9383
CVE-2020-10029 CVE-2020-10531 CVE-2020-10690 CVE-2020-10711 CVE-2020-10713
CVE-2020-10751 CVE-2020-10757 CVE-2020-10942 CVE-2020-11494 CVE-2020-11565
CVE-2020-11608 CVE-2020-11609 CVE-2020-11668 CVE-2020-11669 CVE-2020-11884
CVE-2020-11931 CVE-2020-11935 CVE-2020-12049 CVE-2020-12114 CVE-2020-12243
CVE-2020-12399 CVE-2020-12400 CVE-2020-12401 CVE-2020-12402 CVE-2020-12464
CVE-2020-12652 CVE-2020-12653 CVE-2020-12654 CVE-2020-12657 CVE-2020-12762
CVE-2020-12769 CVE-2020-12770 CVE-2020-12826 CVE-2020-13143 CVE-2020-13434
CVE-2020-13630 CVE-2020-13632 CVE-2020-13790 CVE-2020-14308 CVE-2020-14309
CVE-2020-14310 CVE-2020-14311 CVE-2020-14416 CVE-2020-14422 CVE-2020-14556
CVE-2020-14577 CVE-2020-14578 CVE-2020-14579 CVE-2020-14581 CVE-2020-14583
CVE-2020-14593 CVE-2020-14621 CVE-2020-15705 CVE-2020-15706 CVE-2020-15707
CVE-2020-15709 CVE-2020-15780 CVE-2020-15861 CVE-2020-15862

- **VTM-42461** Fixed an issue where sometimes a `systemd-timesyncd` process would be running instead of the correctly configured `ntpd`.
- **VTM-42506** Fixed an issue where sysconfig took excessive time to complete when a large number of service discovery pools were configured.

Cloud Platforms

- **VTM-39229** Fixed an issue where NTP would not be correctly configured on appliances running in Azure.

Known Issues in 18.2r2

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 Admin UI **System > 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 **System > 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 Traffic Manager version the rollback version selector on the **System > 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.

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