Release Notes for StarOS™ Software Version 21.19.n3

First Published: August 16, 2020
Last Updated: August 16, 2020

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.19.n2. These release notes are applicable to the VPC-SI and VPC-DI platforms.

NOTE: This 21.19.n3 release is solely intended for customers pursuing ANSSI certification. Please contact your local Sales or Support representative for more information.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.19.n3, build 77052

Descriptions for the various packages provided with this release are located in Release Package Descriptions.

Feature and Behavior Changes

The following features and/or behavior changes have been introduced in this emergency release.

Refer to the *Release Change Reference* for a complete list of feature and behavior changes associated with this software release.

Related Documentation

For a complete list of documentation available for this release, go to http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html.

Installation and Upgrade Notes

This Release Note does not contain installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Firmware Updates

There are no firmware upgrades required for this release.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through the following mechanisms:

■ **Cisco.com Software Download Details:** To find the checksum, hover the mouse pointer over the software image you have downloaded.
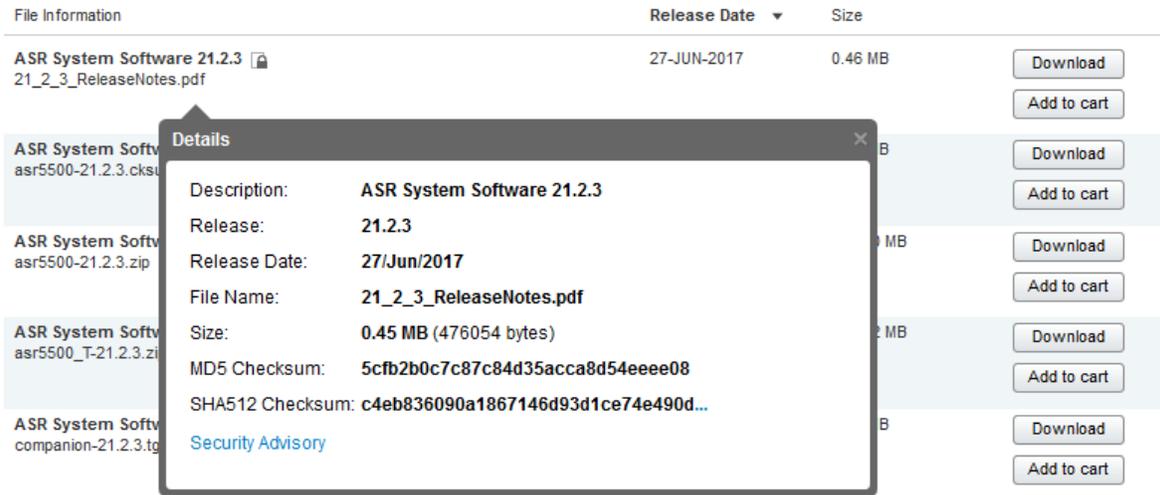
At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

■ **.cksums file:** A file containing software image checksum information is distributed with the image files. The naming convention for this file is:

<product>-<version>.cksums

Example: `asr5500-21.4.0.cksums`

To validate the information, calculate a SHA512 checksum using the information in Table 2 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop please see the table below.

Table 2 - Checksum Calculations per Operating System

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command > certutil.exe -hashfile *<filename>.<extension>* SHA512
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 *<filename>.<extension>*

Operating System	SHA512 checksum calculation command examples

Linux	Open a terminal window and type the following command
	
	$ sha512sum *<filename>.<extension>*
	
	Or
	
	$ shasum -a 512 *<filename>.<extension>*

NOTES: *<filename>* is the name of the file. *<extension>* is the file extension (e.g. .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

In 21.12.0 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates. In pre-21.12.0 releases, image signing is not supported for VPC-DI and VPC-SI images, and for StarOS and VPC companion software packages.

USP ISO images are signed with a GPG key.

For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

Open Bugs in this Release

The following table lists the known bugs that were found in, and/or that remain open in this software release.

NOTE: This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Table 3 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvv15512	[CUPS-CP] ghost UP IDs are present on one CP in ICSR mode	cups-cp
CSCvt26865	sessmgr task restart with fn: sessmgr_ggsn_cups_remove_sx_trans_node()	cups-cp
CSCvv03378	"[BP-CUPS]: sessmgr_ggsn_fill_sub_sess_recovery_info: sgsn gtpu addr NULL callid 99c0d4, "	cups-cp
CSCvu86949	[BP-CUPS]: sessmgr restart at acsmgr_allocate_far_id()	cups-cp
CSCvv17717	[CUPS] UP rejecting calls cause Reporting Triggers not valid	cups-up
CSCvu19385	[BP-CUPS] ICSR - Fatal SIgnal 11 uplane_sfw_nat_gr_handle_nat_realm_update	cups-up
CSCvt15619	[BP-CUPS] : Packet filter list at Uplane is getting corrupted resulting in incorrect rule match	cups-up

Bug ID	Headline	Product Found*
CSCvu00150	[PLT-CUPS]: The p2p app-identifier tls-sni related CLIs failing at UP	cups-up
CSCvu19838	[BP-CUPS] Error Log SEID: Ê Non-zero Correlation id while sending Sx session report request	cups-up
CSCvt97779	"[BP_CUPS] CF: sessmgr recovery when done in a particular sequence, call gets dropped"	cups-up
CSCvu01174	ipsecmgr crash while changing ipsec transform-set hmac config	cups-up
CSCvu14068	[BP_CUPS] : Incorrect i/p o/p data in "sh sub user-plan full all" after SR under specific condition	cups-up
CSCvu19067	'clear crypto statistics' does not clear Combined Data Stats in 'show crypto statistics'	cups-up
CSCvu35075	IPSec SA rekey happens only if 'keepalive' is also configured	cups-up
CSCvu18163	Recovery mechanism is not working as expected for CIOT calls after session manager restart	mme
CSCvu19454	MME doesn't return the UE count in a geographical area when imsi-group is configured in hex-format	mme
CSCvu35147	MONTE: eDRX Device: MME is not sending RIR when UE becomes reachable	mme
CSCvu35160	MONTE: MME sends RIR with a weird AVP User-Name value	mme
CSCvu40373	MONTE: MME doesn't send “Supported-Services” AVP in ISDA S6a	mme
CSCvu70881	[MONTE] Missing AVP 3142 Monitoring-Event-Config-Status in IDA from MME	mme
CSCvu81405	Revert back CSCvr34106	mme
CSCvt79109	"[MONTE]: On PDN Connectivity Status, RIA are not incrementing for detach on scef-service statistics"	mme
CSCvu19517	Maximum-Response-Time AVP is not used as Active Time for PSM	mme
CSCvu20041	Delete counter not incremented proeprly for Monte	mme
CSCvu20206	Loss of connectivity report not triggered for PS to CS SRVCC scenario for Monte with IP PDN	mme
CSCvu20626	[MONTE] bulkstats counter issue for num-of-ues-in-geographical-area	mme
CSCvt47005	[BP-Legacy] Traffic allowed despite CCR failure with FHT continue discard traffic post recovery	pdn-gw
CSCvu05306	"After rekey, IPSec SA Pkts count not reset with IKEv2 SA re-establishment triggered by peer"	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Resolved Bugs in this Release

The following table lists the known bugs that are resolved in this specific software release.

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Table 4 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvu98532	Assertion failure at sess/smgr/sessmgr_ggsn.c	cups-cp
CSCvv13404	[BP-CUPS]: Fatal Signal 11 at sessmgr_is_clp_disconnecting	cups-cp
CSCvu78077	Assertion failure observed on Active saegw cp node at sess/ggsn/app/ggsnapp_db	cups-cp
CSCvu25996	[BP_CUPS]Assertion failure at sessmgr_app_svr_event_control_dispatch()	cups-cp
CSCvu68921	Assertion failure at sess/smgr/sessmgr_gp_handoff on cups control-plane node	cups-cp
CSCvu81900	[PLT-CUPS]: huge CRR recovery failures on back-to-back SRP-Switchover leading to call-drop	cups-cp
CSCvu40586	[PLT-CUPS]: huge CRR recovery failures on back-to-back SRP-Switchover leading to call-drop	cups-cp
CSCvt78639	[BP-CUPS]PC: [045071bc/X] sessmgr_sxu_handle_events_from_egtpu_app()	cups-cp
CSCvu96113	sxmgr-id become 0 after became standby CP node by chassis reload	cups-cp
CSCvu88861	[BP-CUPS] huge number of session disconnects with reason sxfail-opr-get-usagereport	cups-cp
CSCvt88855	AF sess/egtp/egtpc/egtpc_evt_handler_func.c:7432 egtpc_handle_delete_bearer_req_evt()	cups-cp
CSCvu15491	[BP-CUP]S- egtpc_handle_abort_proc_cmd_evt()	cups-cp
CSCvt00492	CUPS-CP : SM crash Fatal Signal 11: Segmentation fault sessmgr_saegw_update_drv_with_sxa_info()	cups-cp
CSCvu38757	[PLT-CUPS]: Many ikev2 CLIs looks failing while configuring	cups-cp
CSCvu38463	Discrepancy at CP on chunks allocated to UP. Unable to bring up calls	cups-cp
CSCvu14812	[CUPS-CP] UPF without chunks triggered even if other UPF with chunks are available	cups-cp
CSCvu44936	CUPS-CP : LTE/WLAN Handover failures due to CP/UP mismatch for the impacted Session	cups-cp
CSCvv15774	npumgr memory leak on UP	cups-up
CSCvu67676	npumgr restart followed by system reload	cups-up
CSCvt85580	VPP Restart and UP reload with rerunning "associate fast-path service" in user-plane-service	cups-up
CSCvu61269	npumgr restart followed by system reload	cups-up
CSCvu93349	[CUPS-UP] IPv6 Fragmented UL ESP packet gets dropped	cups-up
CSCvu73208	[STC CUPS] : Assertion failure at messenger/xdr_msg.c:41	cups-up
CSCvu55658	"[ICSR] Sx Peers are not getting cleared , when peers un-configured after UPswitchover"	cups-up
CSCvu68200	Traffic disturbance when GracefulRestart trigger with ICSR Switchover	cups-up
CSCvu74613	[BP-CUPS] Seg. fault at stat_segment_ls_r()	cups-up
CSCvu69385	[CUPS] [UP] - APN ACL has missing entry on Standby UP after PFD Push from CP	cups-up

| Bug ID	Headline	Product Found*
CSCvu11245	"[sol test] With P2P enabled for a subscriber, the VPP offload toggles between 50% offload and 100%,"	cups-up
CSCvv29752	memory leak in vpp stats client library	cups-up
CSCvr34106	Assertion Failure for aaamgr_sred occurring frequently	mme
CSCvv06146	BP-ICUPS NPUMGR Restart dh_api_get_sockets_handler() sn_msg_arriving_handle() sn_loop_run() main()	pdn-gw
CSCvs38039	VPC-DI | 21.12.0 (71244) | Log rotation is not happening for the iftask_logs file	pdn-gw
CSCvu82604	SF port fluctuation & BFD session keeps on flap	pdn-gw
CSCvt00941	[CUPS]Port flapping occurred continuously on SF node	staros
CSCvq19559	Wrong values on show port utilization table - StarOS VPC-DI	staros
CSCvq92035	[VPC-DI] Excessive packet receive latency on XL710 NICs under no/light load conditions.	staros
CSCvu96129	[VPC-DI/SI] Backport i40evf interrupt handler patch to iftask dpdk 16.07	staros
CSCvt06102	DPC2 memory correctable errors over threshold causing fabric IFMA/Bs	staros
CSCvt89771	[CUPS] [Sx over IPSEC] iftask crash dpdk_app_ucad_op/crypto_handle_req during IKEv2 Tunnel establish	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

StarOS Version Numbering System

The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example "16.1.2".

Pre-16.1

16.0 (65432)

16.1 to 21.0

16.1.[aa]1[.65432]

Major Release Number

Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.

Release Variant Indicator

Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.

StarOS Build Number
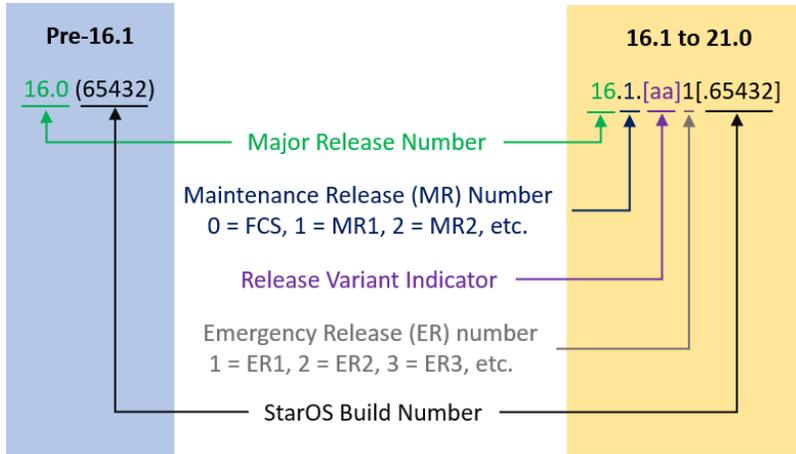
The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".

16.1 to 21.0

16.1.[aa]1[.65432]

21.1 Onwards

21.1.[aa]1[.65432]

Major Release Number

Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.

Release Variant Indicator

Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.

StarOS Build Number
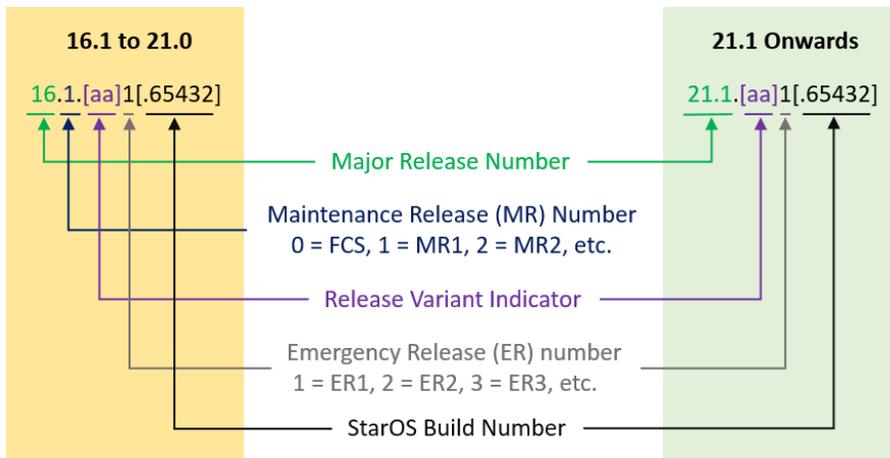
In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 5 provides descriptions for the packages that are available with this release.

Table 5 - Release Package Information

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
ASR 5500		
asr5500-<release>.zip	asr5500-<release>.bin	Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
asr5500_T-<release>.zip	asr5500_T-<release>.bin	Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
StarOS Companion Package		

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
companion-<release>.zip	companion-<release>.tgz	Contains numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants. In 21.12.0 and later releases, the StarOS companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-DI		
qvpc-di-<release>.bin.zip	qvpc-di-<release>.bin	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-vmware-<release>.zip	qvpc-di-template-vmware-<release>.tgz	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-vmware_T-<release>.zip	qvpc-di-template-vmware_T-<release>.tgz	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di-template-libvirt-kvm-<release>.zip	qvpc-di-template-libvirt-kvm-<release>.tgz	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-libvirt-kvm_T-<release>.zip	qvpc-di-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.qcow2.zip	qvpc-di-<release>.qcow2.tgz	Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.qcow2.zip	qvpc-di_T-<release>.qcow2.tgz	Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-SI		
qvpc-si-<release>.bin.zip	qvpc-si-<release>.bin	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.bin.zip	qvpc-si_T-<release>.bin	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.iso.zip	qvpc-si-<release>.iso	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. In 21.12.0 and later releases, the VPC companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at:
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)