Release Notes for StarOS™ Software Version 21.19.n8

First Published: April 23, 2021
Last Updated: April 23, 2021

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.19.n7. These release notes are applicable to the VPC-SI and VPC-DI platforms.

NOTE: This 21.19.n7 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.n8, build 80208

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.
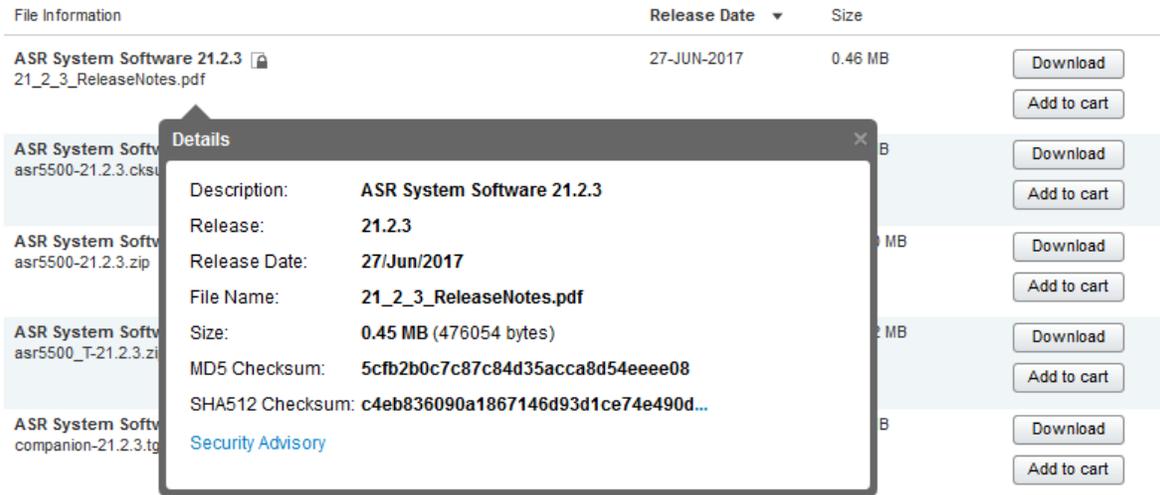
At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

■ **.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*
CSCvu34579	show crypto statistics not display encode and decode data statics in SI and ASR55K	cups-cp
CSCvt26865	sessmgr task restart with fn: sessmgr_ggsn_cups_remove_sx_trans_node()	cups-cp
CSCvx45677	[CUPS] [SGWCDR] - Missing "RANSecondaryRATUsageReport" inside SGWCDR	cups-cp
CSCvu36561	Crash observed on UP at smgr_uplane_update_edr_references_in_all_rbases	cups-up
CSCvw97015	"Sessmgr installing wrong TEP version in VPP, hence packets are dropped"	cups-up
CSCvv14996	[BP_CUPS] Timedef rule matches if no timedef is configured	cups-up
CSCvu01174	ipsecmgr crash while changing ipsec transform-set hmac config	cups-up

Bug ID	Headline	Product Found*
CSCvs05924	[URR] [SXAB] Updated URR doesn't exist	cups-up
CSCvu00150	[PLT-CUPS]: The p2p app-identifier tls-sni related CLIs failing at UP	cups-up
CSCvx64066	IPSec SA rekey happens only if 'keepalive' is also configured	cups-up
CSCvt97779	"[BP_CUPS] CF: sessmgr recovery when done in a particular sequence, call gets dropped"	cups-up
CSCvu14090	[BP-CUPS] sessmgr restart at add_chunk() function	cups-up
CSCvu19385	[BP-CUPS] ICSR - Fatal SIgnal 11 uplane_sfw_nat_gr_handle_nat_realm_update	cups-up
CSCvu35075	IPSec SA rekey happens only if 'keepalive' is also configured	cups-up
CSCvu35147	MONTE: eDRX Device: MME is not sending RIR when UE becomes reachable	mme
CSCvu70881	[MONTE] Missing AVP 3142 Monitoring-Event-Config-Status in IDA from MME	mme
CSCvu81405	Revert back CSCvr34106	mme
CSCvu67421	MONTE : MSISDN value is wrongly enclosed into User-Name AVP instead of MSISDN AVP in RIR message	mme
CSCvu19454	MME doesn't return the UE count in a geographical area when imsi-group is configured in hex-format	mme
CSCvu40373	MONTE: MME doesn't send 'Supported-Services' AVP in ISDA S6a	mme
CSCvu18163	Recovery mechanism is not working as expected for CIOT calls after session manager restart	mme
CSCvu20041	Delete counter not incremented proeprly for Monte	mme
CSCvu70861	[MONTE] RIR is not sent in case if eDRX activated not during Attach but in TAU	mme
CSCvv34694	Sessmgr restarts seen at mme_hss_checkpoint_internal	mme
CSCvu20206	Loss of connectivity report not triggered for PS to CS SRVCC scenario for Monte with IP PDN	mme
CSCvq71949	Task restart while handling li session	mme
CSCvu69504	sessmgr restart occurred at diabase_peer_conn_res_info	mme
CSCvx23843	MONTE: S6a IDR NPC timers not sent to T6a in RIR and not sent to UE in TAU_ACCEPT	mme
CSCvu20626	[MONTE] bulkstats counter issue for num-of-ues-in-geographical-area	mme
CSCvu35160	MONTE: MME sends RIR with a weird AVP User-Name value	mme
CSCvw03127	Frequent sessmgr restart on acs_flush_ttl_aged_entries_from_ip_pools	pdn-gw
CSCvw76775	Many sessmgr restarts seen on virtual PGW	pdn-gw
CSCvg20133	Segmentation fault at PC: [0d8e2647/X] EZprmSER_CheckError()	staros
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*
CSCvy02620	[CUPS] [PGWCDR] - causeForRecClosing set to "Normal Release" when Sx Path Failure occurs in 3G/2G	cups-cp
CSCvx72095	[BP-CUPS]: SessMgr restart @ sessmgr_snx_send_drop_call()	cups-cp
CSCvx74438	TCP state is INACTIVE in the output of the CLI 'show lawful-intercept full imsi xx' on CP side	cups-cp
CSCvw99517	[CUPS] Unexpected combinations of CRBN value and PLMN value in CDRs	cups-cp
CSCvx45708	[CUPS] [PGWCDR] - causeForRecClosing set to "Normal Release" when Sx Path Failure occurs	cups-cp
CSCvx56945	[BP-CUPS] CDR not getting generated upon context replacement	cups-cp
CSCvx59968	CP sends wrong APN-AMBR (MBR) in QER in PFCP session modification request messages	cups-cp
CSCvx62382	[CUPS-CP] Stale session on CP after Gx rule install failure in 3G	cups-cp
CSCvu48856	[BP-CUPS]: [gtpc 47514 error] GTPC Misc error: Deactivation already in progress.	cups-cp
CSCvx69017	Assertion failure at sess/smgr/sessmgr_saegw.c:8912 @ Function: sessmgr_delete_pending_timeout()	cups-cp
CSCvx54858	[CUPS CP] GGSN sends CPC Response with Tunnel ID Data I: 0x00000000	cups-cp
CSCvw70626	UE is not on CP but on UP causing DLDR session report rejection from CP	cups-cp
CSCvw27942	[Smoke2-Legacy] show acs session charging update RG state "Final Unit"	cups-cp
CSCvx08962	[CUPS SX] - Unexpected "LINKED URR ID" value (0x00000000) after Rulebase Change	cups-cp
CSCvx73933	CUPS UP - Packets stuck in VPP queue during OOO condition if stream is in config/pre-active state	cups-up
CSCvw77581	[BP-CUPS] ruledef priority change and sx config push results in peering loss and outage	cups-up
CSCvx32800	[BYTEL / CUPS / UPF-DATA] LOAD TESTING	cups-up
CSCvt89273	CUPS-UP : 'show subscribers all' starOS CLI command causes Sessmgr task restarts	cups-up
CSCvu19838	[BP-CUPS] Error Log SEID: Non-zero Correlation id while sending Sx session report request	cups-up
CSCvs30808	[BP-CUPS] calls disconnected with reason graceful-cleanup-on-audit-fail after srp switchover	cups-up
CSCvw54270	CUPS sessmgr restart on UPFData sessmgr_connproxy_client_state_cb	cups-up
CSCvx80308	[BP-ICUPS]:SM restart observed on active/standby with plain callmodel	pdn-gw
CSCvu61088	Traffic drop in certain SF cards after Nexus switch multi port failures	pdn-gw

Bug ID	Headline	Product Found*
CSCvv52504	PGW not setting the IPv6 Layer Hop Limit	pdn-gw
CSCvw77989	Sessmgr restart while processing Secondary RAT Usage CDR records #2	pdn-gw
CSCvq31796	[BP-ICUPS] Incorrect session count under "show gtpu stat"	pdn-gw
CSCvu51831	Not all sessmgrs came up after upgrading to 21.15.37.75871	pdn-gw
CSCvw64863	[Smoke2-Legacy] TCP FIN/Reset are not sent post readdress rule install.	pdn-gw
CSCvv21979	[VPC] sw-rss does not handle ipv4 packets correctly that introduces out of order packets	staros
CSCvx07298	[CUPS / UPF / OAM / SR-IOV] Bonding not working	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".
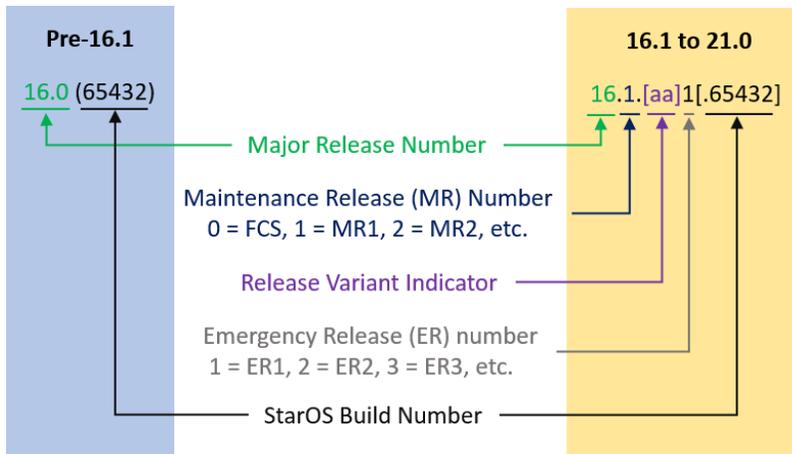
The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".
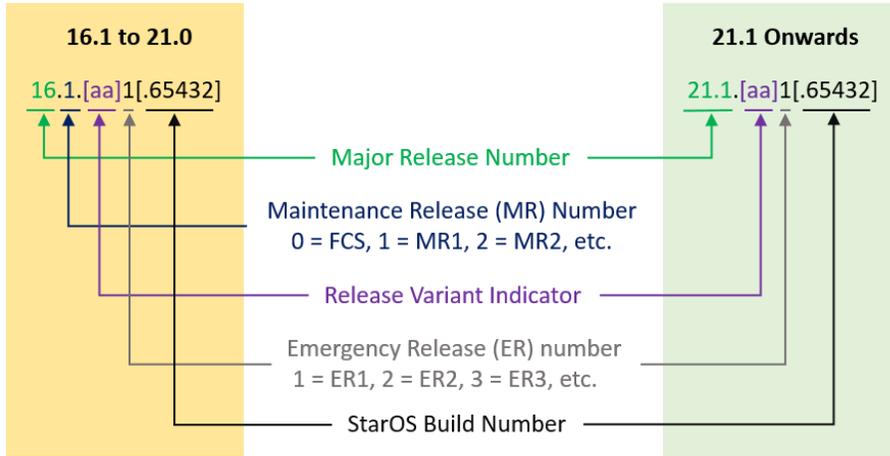
In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using 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		
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.