Known Issues

For your convenience, the release notes list the known issues for major releases. We do not list known issues for maintenance releases or patches.

If you have a support contract, you can use the Cisco Bug Search Tool to obtain up-to-date bug lists. You can constrain searches to bugs affecting specific platforms and versions. You can also search by bug status, bug ID, and for specific keywords.

Important Bug lists are auto-generated once and are not subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. You should regard the Cisco Bug Search Tool as the source of truth.

Version 6.2.3 Known Issues

Table 1: Version 6.2.3 Known Issues

Bug ID	Headline
CSCvf16001	SF Cli - "inside" or "outside" interface capture not giving all options
CSCvh73096	Firepower Management Center does not support userPrincipalName attribute for login with ISE 2.2+
CSCvh89068	Core in Firepower Management Center Perl
CSCvh95960	Using the match keyword in capture command causes IPv6 traffic to be ignored in capture
CSCvi07656	Small number of TLS connections can fail after TLS inspection in Hardware Mode is overloaded
CSCvi10758	With SSL inspection in software mode, a few TLS connections fail to close in a timely manner
CSCvi16024	SSL errors on session resume when server IP address changes - HW mode

Bug ID	Headline
CSCvi18123	Firepower Threat Defense show tech-support command output broken on 2100 from CLISH CLI
CSCvi19862	With SSL inspection enabled, TLS traffic throughput can drop following high-availability failover
CSCvi35176	Deployment Failed-Snort Restart Failure-APPLY_APP_CONFIG_APPLICATION_FAILURE SignalAppConfigFailed
CSCvi35588	Deployment failure due to Snort failed to restart PDTS Handle was NULL
CSCvi42539	Decrypted connections fail when SSLv2 is supported but a higher version is negotiated
CSCvi47264	Some indicators may stay pending when consuming TAXII feeds in parallel
CSCvi49538	Firepower Device Management fails on 2100 (6.2.3-51 (PortChannel))
CSCvi50731	Unable to delete certificate objects if there were previous used at ISE even it was deleted
CSCvi61411	Routed Threat Defense allows Transparent Configuration, but traffic fails (6.2.3-66) on KVM only
CSCvi62982	Firepower Threat Defense virtual on ESXi Firstboot config does not sync hostname correctly with FQHN
CSCvi63157	Firepower 2110 dropping connections
CSCvi63864	With SSL inspection in hardware mode and Malware protection, secure file transfers occasionally fail
CSCvi66189	CNP has been enabled in Firepower Management Center where it usage Satellite server for license
CSCvi70680	Same groups from different AD not downloaded
CSCvv14442	FMC backup restore fails if it contains files/directories with future timestamps