

Dear Cisco Customer,

Cisco engineering has identified the following software issues with the release that you have selected that may affect your use of this software. Please review the Software Advisory notice here to determine if the issues apply to your environment. You may proceed to download this software if you have no concerns with the issue described.

For more comprehensive information about what is included in this software, refer to the Cisco software Release Notes, available from the [Product Selector tool](#). From this page, select the product you are interested in. Release Notes are under "General Information" on the product page.

Affected Software and Replacement Solution for CSCvu65843		
Software Type	Software Affected	Software Solution
Cisco FXOS with FTD on Firepower 2100 devices	Version: Firepower 6.6 Affected Images: Cisco_FTD_SSP_FP2K_Upgrade-6.6.0-90.sh.REL.tar cisco-ftd-fp2k.6.6.0-90.SPA	Version: Firepower 6.6.0.1 Replacement Images: Cisco_FTD_SSP_FP2K_Patch-6.6.0.1-7.sh.REL.tar

Reason for Advisory:

This software advisory addresses one software issue.

CSCvu65843

FP2100: Fiber SFP Interfaces down due to autonegotiation changes in 6.6.0

Affected Platforms:

Firepower 2100 series devices, when using 1GE Fiber SFPs

Symptom:

1 GE SFP Interfaces are in a down state once running FTD 6.6.0

Conditions:

Firepower 2100 series devices running 6.6.0, using 1GE Fiber SFPs (in eth1/13+ ports).

Workaround:

Note: If for any reason the peer device negotiation configuration cannot be adjusted, contact TAC for a temporary alternative workaround. Note that this alternative workaround will not persist through policy deployments, and cannot be done until after FMC registration.

Standalone:

1. Start the upgrade for the FTD. For more information about the FTD upgrade process, see:
https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpm-c-upgrade-guide/upgrade_firepower_threat_defense.html#id_59714
2. SSH to the device. In the FTD CLI, enter 'expert' to get to expert mode:
expert

NOTICE - Shell access will be deprecated in future releases
and will be replaced with a separate expert mode CLI.
admin@<hostname>:/\$
3. In the expert mode CLI, run 'cd /ngfw/var/log/sf/'
admin@<hostname>:/\$ cd /ngfw/var/log/sf/
admin@<hostname>:/ngfw/var/log/sf\$
4. In this directory – wait until the 'patch/upgrade' directory shows up - run the 'ls' command every few seconds to see when the directory is created.
Example:
admin@<hostname>:/ngfw/var/log/sf\$ ls
VDB_update_info.txt data_service.log policy_deployment.log sru-2018-10-10-001-vrt
update.status vdb-4.5.0-309 verify_file_integ.log verify_signature.log

admin@<hostname>:/ngfw/var/log/sf\$ ls
Cisco_FTD_SSP_FP2K_Upgrade-6.6.0 VDB_update_info.txt data_service.log policy_deployment.log
sru-2018-10-10-001-vrt update.status vdb-4.5.0-309 verify_file_integ.log
verify_signature.log
5. Once the Upgrade/Patch directory is created, the upgrade can be monitored by running the following command:
'tail -f <name of upgrade dir>/main_upgrade_script.log'
Example:
admin@<hostname>:/ngfw/var/log/sf/\$ tail -f Cisco_FTD_SSP_FP2K_Upgrade-6.6.0/main_upgrade_script.log
6. Watch the output of the above command and wait until the log goes past 'END 200_pre/200_enable_maintenance_mode.pl'
Example:
[200714 07:05:01:690] BEGIN 200_pre/199_before_maintenance_mode.sh
[200714 07:05:02:258] END 200_pre/199_before_maintenance_mode.sh
[200714 07:05:02:364] BEGIN 200_pre/200_enable_maintenance_mode.pl
[200714 07:05:06:928] END 200_pre/200_enable_maintenance_mode.pl
7. Once the log is past the "END 200_pre/200_enable_maintenance_mode.pl" phase, run the 'no negotiate auto' command to disable auto negotiation on the peer switch 1GE fiber link ports connected to the device.
Example:
switch (config)# interface ethernet 1/38

switch (config-if)# no negotiate auto

8. Let the rest of the upgrade finish – you can leave the device CLI in expert mode. The device should reboot and the 1GE fiber ports should come up as per configured admin-state.

HA Pair:

1. Start the upgrade for the FTD. For more information about the FTD upgrade process, see:
https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpm-c-upgrade-guide/upgrade_firepower_threat_defense.html#id_59714
2. The standby device in the HA pair will upgrade first.
3. On the standby device, run steps 2-8 from the Standalone workaround procedure, above.
4. Once the Standby unit has rebooted completely, it will rejoin the HA pair. Once it has rejoined HA pair, switch over to the Active device and monitor the state of the failover using ‘show failover state’ from the FTD CLI.
5. The state of the upgraded unit should eventually move to ‘Standby Ready’ in the ‘show failover state’ output:

> show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Bulk Sync	Comm Failure	12:47:19 UTC Jul 14 2020

> show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	Comm Failure	12:47:19 UTC Jul 14 2020

6. Once the Secondary is at ‘Standby Ready’, the HA pair has reconnected. The upgrade on the Active unit will begin automatically.
Note: During the “200_pre/200_enable_maintenance_mode.pl” upgrade phase, a failover between the FTDs will occur – this is expected behavior for FTD upgrades in order to avoid downtime from the upgrade process.
7. Now on the (previously) Active unit that is upgrading, run steps 2-8 from the Standalone workaround procedure, above.

Fix Release Vehicle Plans

This issue is fixed in patch 6.6.0.1, as well as in our next maintenance release - 6.6.1. The 6.6.1 maintenance release is targeted to release in the second half of calendar year 2020.

The fix will revert the changes made in 6.6.0 and restore the behavior in version 6.5 and earlier, where auto-negotiation was enabled for Firepower 2100 device interfaces. Note that if you perform the workaround on 6.6.0 to disable auto-negotiation [switch(config-if)# no negotiate auto], when you upgrade to 6.6.0.1, you must revert the workaround to re-enable auto negotiation [switch(config-if)# negotiate auto].