Brocade FOS Release v7.2.0d6 Internal Content Notes

The Brocade CCE process has been used to provide stable code fixes to various Brocade customer sites. This CCE has been created especially for FICON customers that require at a minimum the IBM FICON qualified FOS V7.2.0d code base with important fixes. This CCE is based off the IBM FICON Qualified FOS release of V7.2.0d plus confirmed changes.

The following sections document the defects and improvements that have been fixed in this release. CCE Builds are available to customer sites through an SR Request to Brocade Support.

CCEs are packaged exactly the same way as a normal Brocade FOS Release. The normal Firmware Download process is used to upgrade a switch to the CCE.

This document can be shared with customers and partners as required. The following sections include the list of Defects and descriptions of the issues that have been incorporated into this release as well as those ported from the listed CCE releases.

Common Questions and Answers Related to the Bash Shell Security Vulnerability Fix (Defect 529761)

Q How is FOS exposed to the Bash Shell security vulnerability?

A FOS is only exposed when an authenticated user login to a Brocade switch and gain access to the CLI interface. This includes login through Console, Telnet, SSH connections. An authenticated user account could exploit this vulnerability to gain privileges beyond the permission granted to the account, such as executing commands with root privilege.

FOS is not exposed to the Bash Shell vulnerability through remote attacks, specifically through any of the following protocols.

- SNMP – not exposed. FOS does not support executing shell script.
- SMI-S – not exposed. FOS does not support executing shell script.
- HTTP – not exposed. FOS does not allow arbitrary code / scripts (CGI) to run**.**
- DHCP client – not exposed. FOS does not support DHCP script capabilities. FOS DHCP client does not support option 114.

Q How can I mitigate the Bash Shell vulnerability in FOS?

A Following is a list of mitigation procedures to strengthen Brocade switch account management and hence remove the exposure to the Bash Shell vulnerability.

- Place your Brocade SAN switch and other data center critical infrastructure behind firewall to disallow access from the Internet.
- If you have not done so in the past, change all Brocade default account passwords, including the root passwords, from the factory default passwords.
- Examine the list of accounts, including the ones on the switch and ones on remote authentication servers, such as RADIUS, LDAP, and TACAS+, to ensure only the necessary

personnel are granted access to Brocade FOS switch. Delete guest accounts and temporary accounts created for one-time usage.

- Utilize FOS password policy management to strengthen the complexity, age, and history requirements of switch account passwords.

Q Do I have to install this CCE patch to mitigate the Bash Shell vulnerability in FOS?

A If you have followed the mitigation procedures documented above to protect your switch accounts, it is not necessary to install this CCE patch. You can wait for the next scheduled upgrade to a supported patch version that contains the fix to the Bash Shell vulnerability, ideally to a FOS Target Path release.

Please note, once upgraded, if you want to download to a release without the Bash fix again, you may see some Bash error during firmware cleanup as part of the firmware download process. These can be ignored and will be cleaned up again in future upgrades to a release with the Bash fix.

```
###############################

Removing unneeded files, please wait ...
There was a problem cleaning /bin, retrying
There was a problem cleaning /bin, retrying
There was a problem cleaning /bin, retrying
There was a problem cleaning /sbin, retrying
There was a problem cleaning /sbin, retrying
There was a problem cleaning /sbin, retrying
```

v7.2.0d6 was completed on 10/9/2014

Defect ID:	DEFECT000529761		
Technical Severity:	High	**Probability:**	Medium
Product:	FOS	**Technology:**	Security
Reported In Release:	FOS6.3.0	**Technology Area:**	Security Vulnerability
Closed In Release(s):	FOS6.2.2f9, FOS6.4.2a1, FOS6.4.3f3, FOS 7.0.0d1, FOS7.0.2e1, FOS7.1.0cb, FOS7.1.1c1, FOS7.1.2b1, FOS7.2.0d6, FOS7.2.1c1, FOS7.3.0b		
Symptom:	Bash shell security vulnerabilities (CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187). The vulnerability allows certain malformed function definition to bypass privilege boundaries and execute unauthorized commands.		
Condition:	To exploit this vulnerability in FOS requires access to the CLI interface after user authentication through console, Telnet, and SSH connections. An authenticated user account could exploit this bug to gain privileges beyond the permission granted to this account, such as executing commands with root privilege.		
Workaround:	Place switch and other data center critical infrastructure behind firewall to disallow access from the Internet; Change all default account passwords; Delete guest accounts and temporary accounts created for one-time usage needs; Utilize FOS password policy management to strengthen the complexity, age, and history requirements of switch account passwords.		

v7.2.0d5 was completed on 09/19/2014

Defect ID: DEFECT000527848	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0d	**Technology Area:** FCIP
Closed In Release(s): FOS7.1.0cb, FOS7.2.0d5, FOS7.4	
Symptom: VM SPOOL DUMP FICON emulated Tape backup jobs fail after FOS upgrade	
Condition: After upgrading to FOS v7.2.0d, when using FICON Tape Emulation for VM tape operations	
Workaround: Disable FICON Tape Emulation on the FCIP Tunnel or downgrade to a FOS version without fix for TR 414719	

v7.2.0d4 was completed on 09/02/2014

Defect ID: DEFECT000526447	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0d	**Technology Area:** FCIP
Closed In Release(s): FOS7.1.0cb, FOS7.2.0d4, FOS7.3.0b	
Symptom: FX8-24 or 7800 FCIP DP complex slow FCIP throughput	
Condition: Configurations with multiple very active FCIP Tunnels on a 7800 or FX8-24 FCIP DP complex	
Workaround: None – can occur based upon internal flow control events	
Recovery: Power cycle (slotpoweroff/on) slot or reset chassis	

Defect ID: DEFECT000525406	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.0.0	**Technology Area:** Other
Closed In Release(s): FOS7.2.1c, FOS7.2.0d4, FOS7.3.0b	
Symptom: When customers configure Edge Hold Time (EHT) in 16G switches running FOS v7.0.0, F-port and E-port do not get expected values.	
Condition: It happens when a user makes EHT change on a 16G switch running FOSv7.0.0. FOS v7.1, v7.2 and v7.3 do not have this problem. But upgrading to these releases does not automatically correct the condition caused by FOS v7.0.0.	
Recovery: Upgrade to a release containing this fix, and re-run configure command to set the correct EHT values. Alternatively, run slotpoweroff/on if the switch has already been upgraded to FOS v7.1 and above.	

v7.2.0d3 was completed on 08/15/2014

Defect ID: DEFECT000508529	
Technical Severity: Critical	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.0c	**Technology Area:** Trunking
Closed In Release(s): FOS7.2.0d3(Fixed)	
Symptom: High deskew values on 16G trunk ports are contributing to high fabric latency.	
Condition: It occurs during trunk forming with 16G ports. Sometimes the impact is not observed until after a hafailover/hareboot. trunkshow shows huge deskew value difference between links in a single trunk. Example of an actual trunkshow output of a high latency fabric: trunkshow : 1: 0-> 0 xxx deskew 1517 MASTER 1-> 1 xxx deskew 15	
Workaround: port disable and enable links in the trunk one by one: portdisable link1, portenabel link1; portdisable link2; portenable link2.	

Defect ID: DEFECT000511932	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** Zoning
Closed In Release(s): FOS7.2.0d3(Fixed)	
Symptom: Observed "[SCN-1001], 19909, SLOT 4 | FFDC | CHASSIS, CRITICAL, , SCN queue overflow for process nsd" on standby CP.	
Condition: It happens when there are enough zone updates done on the system.	
Workaround: No functional impact. Reboot standby CP to clear it up.	

Defect ID: DEFECT000512057	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.2.0b	**Technology Area:** Fabric Watch
Closed In Release(s): FOS7.2.0d3(Fixed)	
Symptom: Error messages start after firmware update from FOS v7.0.x to FOS v7.1.x and continue when upgrading to FOS v7.2.x. After downgrading back to 7.0.x, faulty port messages stop from Fabric Watch.	
Condition: Running FOS 7.1 and above, with a port remains in passive mode, which would simply complete speed negotiation and failing link init, results in FW-xxxx flood in RAS log.	
Workaround: Disable the port that does not cut off light.	

v7.2.0d2 was completed on 07/29/2014

Defect ID: DEFECT000361971	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.0.0	**Technology Area:** Other
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: F-Port was logged out of switch due to laser fault during media access.	
Condition: This is an unlikely situation that may be encountered under heavy CPU load and rare timing race condition. i2c read of smart data has been enhanced to address this for impacted CPU type.	

Defect ID: DEFECT000464907	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS6.1.0_utah	**Technology Area:** Other
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: A misbehaving device continuously sending switch size 0 frames cause switch to panic.	
Condition: A misbehaving device continuously sending size 0 frames to switch 5481.	

Defect ID: DEFECT000470985	
Technical Severity: Low	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS6.4.3e	**Technology Area:** Other
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Customer request to change i2c media thread priority to 10 as default	

Defect ID: DEFECT000472904	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0a	**Technology Area:** FC-FC routing
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: 16G ASIC signal equalizer (DFE) running at 8G may drift due to IDLE fill words received resulting in CRC errors and server tapes not accessible after reboot.	
Condition: This may be encountered when 16G ASIC speed negotiates or is locked at 8G.	

Defect ID: DEFECT000473940	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2b	**Technology Area:** Routing
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: After upgrading from v6.4.3b to v7.0.2c several ports observed C2-1013 (Duplicate rte_tbl_select detected!) messages.	
Condition: The C2-1013 messages are harmless and might be seen after an firmware download from FOS v6.4.3b to v7.0.2c.	

Defect ID: DEFECT000477834	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0c1	**Technology Area:** OSTP - Open Systems Tape Pipelining
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: In an FCIP tunnel using OSTP, tape server reports intermittent missing block errors.	
Condition: During error recovery for FC CRC errors, OSTP may incorrectly send frames out of order.	

Defect ID: DEFECT000477917	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS6.4.3b	**Technology Area:** Routing
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Spinfab fails across TI Zone when link cost is higher than that of normal E-ports.	
Condition: Testing ports bounced after link cost was changed to a higher than normal traffic E-ports between the same two domains.	
Workaround: Change the link cost without bouncing the port.	

Defect ID: DEFECT000482227	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0a	**Technology Area:** CLI
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: 'portdecom' command on a port displays "Error: Request failed due to the local port not being in a ready state" message	
Condition: Occurs when 'portdecom' command runs on a trunk slave port that is connected to port index zero (0) on one end of the link and it is disabled already.	
Workaround: Do not issue 'portdecom" command on a disabled port.	

Defect ID: DEFECT000484414	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.2c	**Technology Area:** Access Gateway
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Under rare conditions, Access Gateway(AG) entries stay in management server (MS) database even after removing them from the fabric.	
Condition: This may be observed on a switch running firmware version higher than v7.0.	

Defect ID: DEFECT000489686	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Disk to disk backups from site to site are failing. Multiple internal ports on FX8-24 appear to have persistent -3 credit on data VC.	
Condition: A rare FPGA issue, that loops back a buffer before filling it with new FC data frames, may cause VC credit depletion.	

Defect ID: DEFECT000491841	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0b	**Technology Area:** Lossless DLS
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: When F-port trunking is enabled, portdecom on the E-port may fail with "invalid remote port type".	
Condition: This portdecom failure on the E-port may be encountered when F-port trunking is enabled.	
Workaround: Disable F-port trunking, then portdecom will work.	

Defect ID: DEFECT000499895	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Uncompressed throughput on the 10GE FCIP complex drops to about 52M/Sec and never recovers.	
Condition: If some TCP connections had byte flow control indicated and others had PDU flow indicated, this could lead to a TX stall in FCIP Tunnel processing.	
Workaround: Start and stop FCIP Tunnel traffic.	

Defect ID:	DEFECT000502591		
Technical Severity:	High	**Probability:**	Low
Product:	FOS	**Technology:**	Traffic Management
Reported In Release:	FOS7.2.0b	**Technology Area:**	Routing
Closed In Release(s):	FOS7.2.0d2(Fixed)		
Symptom:	On a switch that had pre-FOS v7.1 installed before, upgrade the switch to FOS v7.1 or later, host lost access to storage with missing route.		
Condition:	If there is a port bounces during hareboot/hafailover (or as part of firmwaredownload), switches could see this problem.		
Workaround:	Upgrade to a release containing defect 459831 fix (FOS v7.1.1a, v7.1.2, v7.2.0). If a later release is needed, then upgrade must be done to a release with the fix to this defect in it.		

Defect ID:	DEFECT000503299		
Technical Severity:	High	**Probability:**	Low
Product:	FOS	**Technology:**	Other
Reported In Release:	FOS6.4.3e	**Technology Area:**	Other
Closed In Release(s):	FOS7.2.0d2(Fixed)		
Symptom:	After FOS upgrade, CLI "switchshow" reports multiple ports in disabled state with reason as "Not ready for F or L ports", "Switch not ready for EX_Ports"		
Condition:	Occasionally, switch finds inconsistency in domain count and E-port count during HAfailover/hareboot when there is VEX-EX ports in the configuration.		

Defect ID:	DEFECT000503458		
Technical Severity:	High	**Probability:**	Medium
Product:	FOS	**Technology:**	Monitoring/RAS
Reported In Release:	FOS7.3.0	**Technology Area:**	Flow Vision: Flow Generator
Closed In Release(s):	FOS7.2.0d2(Fixed)		
Symptom:	Switch is still operational but HA is out of sync. Reboot switch cannot bring HA Sync back. Any Flow Vision (Flow Monitor, Flow Mirror and Flow Gen) operations fail.		
Condition:	In a Port Based Route (PBR) or Device Based Routing (DBR)environment and customer has configured two or more Flow Gen.		
Workaround:	Do not configure more than 1 Flow Gen in PBR/DBR setup		

Defect ID: DEFECT000512507	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.2.0	**Technology Area:** Routing
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Observed performance issue on FX8-24 when there are exactly two equal bandwidth FCIP tunnels.	
Condition: Only applicable when there are two incoming paths (E-ports, trunks, EX-ports) on a given FX8-24 or BR7800 ASIC Chip.	
Workaround: Use one or greater than two incoming path to FX8-24 and 7800, or configure one of the links with a slightly lower bandwidth.	

Defect ID: DEFECT000513920	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS7.1.0a	**Technology Area:** Fabric Authentication
Closed In Release(s): FOS6.4.3f2, FOS7.0.0d1, FOS7.0.2d6, FOS7.0.2e1, FOS7.1.0cb, FOS7.1.1c1, FOS7.1.2b, FOS7.2.0d2, FOS7.2.1b, FOS7.3.0	
Symptom: CVE-2014-0224: OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	
Condition: FOS switches that are not running LDAP or RADIUS with PEAP-MSCHAPv2 for authentication are not running OpenSSL client mode and are not at risk. To be at risk: • The FOS product must be running authentication using LDAP or RADIUS with PEAP-MSCHAPv2 protocols. • The OpenSSL server must also be running with a version of OpenSSL that contains this vulnerability (1.0.1 or 1.0.2-beta1)	
Workaround: For users requiring LDAP or RADIUS with PEAP-MSCHAPv2 for authentication, upgrading the OpenSSL server to a version of OpenSSL that does not contain this vulnerability will prevent exposure.	

Defect ID: DEFECT000515486	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.1c	**Technology Area:** Other
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Director panic due to software watchdog timeout with pdmd daemon. Prior to the panic, switch logged repeat message: "FSS Error: pdm: not acked!"	
Condition: This happened after the standby CP was "REMOVED".	

Defect ID: DEFECT000516599	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: XTUN-1008 messages reported every 5 minutes in the RAS log and BNA console.	
Condition: After extended uptime in a large FCIP FCP Fast Write and Open Systems Tape Pipelining configuration.	
Workaround: Reboot FCIP switch or power cycle the slot that is reporting the messages.	

Defect ID: DEFECT000516703	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0c	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: FICN-1062 and FICN-1063 abort messages on XRC and IFCC on host.	
Condition: In a large FICON disk mirroring configuration that includes base and alias devices in the connected primary controllers.	

Defect ID: DEFECT000518620	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS7.2.1a	**Technology Area:** Other
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Detect 400K CRC errors with good EOF on backend C-port. Md demon terminated with ASSERT.	
Condition: This happens when MAPS and Auto tuning are enabled at the same time.	
Workaround: Avoid using MAPS and Auto-tuning at the same time.	

Defect ID: DEFECT00521195	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.2.0	**Technology Area:** FICON
Closed In Release(s): FOS7.2.0d2(Fixed)	
Symptom: Able to configure IDID to ON while the switch is online to make upgrading from v7.2.x to v7.3 non-disruptive.	
Condition: Without this fix, setting IDID ON would require switchdisable.	

v7.2.0d1 was completed on 4/4/2014, and includes the fixes for the following defects:

Defect ID: DEFECT000461189	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** Web Tools
Closed In Release(s): FOS7.2.0d1(Fixed)	
Symptom: Unable to launch WebTools using Google Chrome browser and IE11 with Java update 45 or 51	
Condition: This happens when using the latest Java update revision 45 or 51.	
Workaround: Use another browser or older Java update.	

Defect ID: DEFECT000462116	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Director rebooted: CPs lost heartbeat and active CP was reset, standby CP panicked during take over.	
Condition: Port blade hardware failure may trigger loss of heartbeat (between two CPs).	
Recovery: Switch is recovered after reboot; replace bad port blade to prevent re-occurrence..	

Defect ID: DEFECT000477948	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Toggling autoneg on a disabled ge port then reenabling it will sometimes have other ge ports going to 'no sync' state as a result	
Condition: General procedure: 1. portdisable ge port 2. portcfg autoneg <ge port> --disable 3. portcfg autoneg <ge port> --enable 4. portenable <ge port> Then note that a different ge port goes to 'No_Sync' status	
Workaround: Use portdisable/portenable alone.	

Defect ID: DEFECT000483044	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0c	**Technology Area:** Extended Fabrics
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Failed disk copy MVS jobs	
Condition: This may be encountered when zHPF is enabled	
Recovery: Restart switch with zHPF disabled	

Defect ID: DEFECT000487895	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.1	**Technology Area:** Web Tools
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Even after java is updated, when launching WT from IE11, browser reports java has to be updated	
Condition: This is encountered when launching Webtools from IE11.	
Workaround: Use a different browser.	

Defect ID: DEFECT000492849	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.1	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: FCIP link became unstable after some run time and reported the following XTUN messages: 2014/02/03-09:50:40, [XTUN-1008], 12759, CHASSIS, WARNING, , FCIP Control block memory usage slot=0 DP=1 Allocated=5209344 Free=196117248 Total=201326592. 2014/02/03-09:50:41, [XTUN-1001], 12760, FID 128, ERROR, , FCIP Tunnel 16 Memory allocation failed tracker 1/247	
Condition: On switch running with FOS 7.2.0b/c and FOS7.2.1, resource is lost when processing periodic vendor unique message ELS-PRLI coming from a disk mirroring application every 5 seconds.	
Workaround: None.	

Defect ID: DEFECT000454580	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Security
Reported In Release: FOS6.4.2	**Technology Area:** Fabric Authentication
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: With SSL configured on Active CP, a newly inserted Standby CP may panic and go through an unnecessary additional reboot.	
Condition: When SSL configured in the active CP, inserting a new standby CP whose time is later than that of Active CP & don't have SSL configured already can cause a panic & unnecessary additional reboot of standby CP after insertion.	
Workaround: Insert standby CP with hadisabled state. Login to standby CP, change standby CP's date to earlier than that of the active CP using "/bin/date" command and then execute haEnable.	
Recovery: No action required. Previous switch reboot will fix the SSL configuration issue.	

Defect ID: DEFECT000462116	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.0	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: Director rebooted: CPs lost heartbeat and active CP was reset, standby CP panicked during take over.	
Condition: Port blade hardware failure may trigger loss of heartbeat (between two CPs)	
Recovery: Switch is recovered after reboot; replace bad port blade to prevent re-occurrence.	

Defect ID: DEFECT000467051	
Technical Severity: Medium	**Probability:** High
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.2	**Technology Area:** Fabric Watch
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: switchstatuspolicy shows incorrect port count which may impact the accuracy of switch status	
Condition: switchstatuspolicy incorrectly accounts for logical ports into the total physical port count.	

Defect ID: DEFECT000468152	**Technical Severity:** High
Summary: after zone change nszonemember missing members and ports show HARD_PORT dhp bit set: 1	
Symptom: A zoning change (removal) was made from the core switch at which time the name server stopped responding, causing outages on the hosts.	
Risk of Fix: Low	
Feature: FOS Software	**Function:** Fabric Services
Reported In Release: FOS7.0.2	**Service Request ID:** 1202661,1249899,7610

Defect ID: DEFECT000474101	
Technical Severity: Critical	**Probability:** Low
Product: FOS	**Technology:** Monitoring/RAS
Reported In Release: FOS7.0.0	**Technology Area:** supportShow
Closed In Release(s): FOS7.1.2(Fixed)	
Symptom: In a virtual fabric environment, a logical port stuck in an invalid/incomplete state triggered a switch panic during a switchshow/supportsave	
Condition: On a rare condition, in a VF environment, if a port is not indexed correctly, subsequent data collection will result in a panic.	

Defect ID: DEFECT000477188	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area:** Platform Services
Closed In Release(s): FOS7.2.1(Fixed)	
Symptom: During hafailover operation, switch reinitializes a port blade due to a false indication of a power (low voltage) issue.	
Condition: An i2c contention during an i2c read/write operation on FC8-48 or FC8-32 port blade, immediately following an hafailover, forces an i2c reset for the corresponding blade.	
Recovery: No further recovery is necessary, data path re-route is already initiated and the FRU re-initialized to remedy the situation.	

Defect ID: DEFECT000477596	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.0.2	**Technology Area:** Web Tools
Closed In Release(s): FOS7.1.2(Fixed)	
Symptom: Weblinker terminated and restarted but could not service the HTTP requests. All requests getting a response "Chassis is not ready for management".	
Condition: On very rare occasions, the issue is seen on switches managed by BNA.	
Recovery: Use hafailover or reboot CLI.	

Defect ID: DEFECT000492340	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.3.0	**Technology Area:** BB Credits
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: May notice frame drops on the back end edge and core ports with FS8-18 and FX8-24.	
Condition: When FS8-18 and FX8-24 blades are used with 16G core blade chassis.	

Defect ID: DEFECT000492854	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Asic Driver
Reported In Release: FOS7.1.0	**Technology Area:** FC-FC Routing
Closed In Release(s): FOS7.1.2(Fixed)	
Symptom: Following a planned device outage, many ports are displayed as FC Disabled (Port Throttled). Ports do not come online for a long time.	
Condition: When a large number of devices with laser on but cannot complete link initialization with switch, and it typically occurs during device power cycle, upgrade, or running diagnostics.	
Workaround: Stage the number of devices coming online at the same time.	
Recovery: Disable the devices that cannot come online to give other ports a chance.	

Defect ID: DEFECT000493752	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON CUP
Closed In Release(s): FOS7.1.2(Fixed)	
Symptom: When there is a Remote CUP, with traffic flowing across 7800 IP links, CUP can become unresponsive.	
Condition: When FICON CUP receives an ELP (Est Logical Path) and that Logical Path already exists, treat the LP as a System Reset for that Logical Path.	
Workaround: Any configuration or process to help avoid this Defect (only for Publication purpose).	

Defect ID: DEFECT000495636	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Other
Reported In Release: FOS7.1.0	**Technology Area:** Other
Closed In Release(s): FOS7.1.2(Fixed)	
Symptom: Switch Panic during CP blade replacement	
Condition: On a very congested switch with lots of BE link resets, the event of bringing down a CP blade may cause a panic condition during the blade shutdown procedure.	
Workaround: Take switch offline and then replace CP blade.	

It also includes merges of a set of CVRs:

Defect Fixed in Release: v7.2.0a_cvr_brcd_466071_01

Defect ID: DEFECT000466071	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Monitor/RAS
Reported In Release: FOS7.2.0	**Technology Area:** Logging
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Observed verify error from name server daemon on an idle switch: "VERIFY - Failed expression: 0, file = ns.c, line = 5834...". Too many verifies can trigger a switch panic	
Condition: When device sent PLOGI with invalid SID/DID, such as SID of 0.	
Workaround: Disable the port connecting to the device sending invalid SID..	

Defect Fixed in Release: v7.2.0a_cvr_brcd_484327_01

Defect ID: DEFECT000484327	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0a	**Technology Area:** FC-FC Routing
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Switch panic after name server detected duplicated WWPN with raslog: 2013/10/22-02:26:59, [NS-1012], 147485, SLOT 6 | FID 128, WARNING, , Detected duplicate WWPN [] - devices removed with PID 0x3ce701 and 0x3ce80	
Condition: This may occur when 1. There is physically duplicated WWPN in the environment, or 2. An interleaved offline and online sequence between two different NPIV ports may trigger a false duplicate WWPN detection.	
Workaround: Remove physically duplicate WWPN devices if any exist..	
Recovery: If there is no physically duplicate WWPN devices, switch recovers itself after panic	

Defects Fixed in Release: v7.2.0c_cvr_brcd_479909_01

Defect ID: DEFECT000465498	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.0a	**Technology Area:** FC-FC Routing
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: FX8-24 failure. Logs indicate fault code rc=2004c, related to power on FX8-24 blade. Logs do not provide fault register data from voltage monitor.	
Condition: This is seen under a rare occurrence of blade fault from power failure.	
Workaround: None.	

Defect ID: **DEFECT00479909**	Technical Severity: High
Summary: Detected termination of process npd" after slotpoweroff all slots and hafailover	
Symptom: Customer may see npd crash after powering off all slots and failover.	

Defect ID: **DEFECT00481199**	Technical Severity: Medium
Summary: Compatibility issues in Web Tools with JRE 7 Update 45	
Symptom: When launching Web Tools a security warning message is displayed.	

Defect ID: **DEFECT00482106**	Technical Severity: Medium
Summary: Ficon “CUE Acc status” times out and is not getting cleared out	
Symptom: The user may see messages about I/O timeouts on the CUP device from host log, or unable to bring the CUP device online.	
Workaround: None	

Defect ID: **DEFECT00486638**	Technical Severity: High
Summary: Ficud terminated and triggered switch panic	
Symptom: Switch panic observed in environment with 8 or more trunk groups.	
Workaround: Reduce trunk group	

Defect ID: **DEFECT00488202**	Technical Severity: High
Summary: FCIP Tunnel bounces with replay checks due to IPSec not rekeying	
Symptom: FCIP Circuit bounces due to replay checks in a setup running IPSec with unidirectional traffic from the lower order IP address to the higher IP address on the circuit	
Workaround: Run uni-directional traffic from the higher order IP address to the lower order IP address on the FCIP circuit.	

Defect Fixed in Release: v7.1.0c_c8

Defect ID: DEFECT000474833	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.0.0	**Technology Area:** FCIP Fastwrite
Closed In Release(s): FOS7.1.2(Fixed)	
Symptom: Job failures after check condition from tape device (the next I/O is incorrectly responded to with a deferred error check condition status).	
Condition: If a tape device is accessed via a non-OSTP (Open Systems Tape Pipelining) tunnel and it returns a check condition to an I/O, FCIP FW processing would incorrectly generate a second check condition status to the next I/O for that tape device.	
Workaround: Enable OSTP on the FCIP FW enabled tunnels if there are also Tape devices accessed via the tunnel.	

Defect ID: DEFECT000477854	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.0.2	**Technology Area:** ICLs - Inter-chassis Links
Closed In Release(s): FOS7.2.0d1(Fixed)	
Symptom: CRC with good EOF errors will be reported on multiple ICL ports in DCX	
Condition: This issue is seen rarely on DCX platforms	

Defect ID: DEFECT000479882	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** FICON
Reported In Release: FOS7.1.0	**Technology Area:** FICON emulation
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Host reported IFCCs due to aborted FICON RRS/Device Level Exception/LACK Sequence	
Condition: If a FICON Disk controller returns a device level exception frame to a read record set CCW command chain, the IFCCs will occur.	
Workaround: Disable XRC Emulation on the FCIP Tunnel	
Recovery: The mainframe will automatically recover from this error.	

Defect ID: DEFECT000484414	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS7.0.2c	**Technology Area:** Access Gateway
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: If system is upgraded to v7.0.2c prior to removing an online AG, then after AG is removed from the fabric, AG still remains as a stale entry in agshow command.	
Condition: The stale AG entries may be encountered if system is upgrade without removing an online AG.	
Workaround: Ensure that AG is removed prior to the upgrade.	

Defect ID: DEFECT000490533	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.1.0c	**Technology Area:** Extended Fabrics
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: FDR (Fast Dump Restore) disk copy MVS jobs fail with zHPF mode enabled.	
Condition: This may occur when zHPF mode is enabled and I/Os include a large number of frames in a FC sequence	
Workaround: disable the zHPF mode	
Recovery: No recovery exists besides restarting the job with zHPF mode disabled	

Defect ID: DEFECT000490548	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.1	**Technology Area:** BB Credits
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Detect CRC error with good EOF on C-port(0) and on C-port(8); This could trigger buffer credit loss on these ports.	
Condition: It happens with Slot 2 port 0 and port 8 of a DCX4s with FC8-48 port cards installed in slot 2.	
Recovery: Manually tune both the port card port and the core blade ports with different values.	

Defect ID: DEFECT000492704	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Traffic Management
Reported In Release: FOS7.1.1	**Technology Area:** BB Credits
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: "CRC error with good EOF" errors detected and may cause credit loss.	
Condition: DCX-4S with FC8-64 blades installed in Slot 7 port 155, 76 Slot 2 port 154. Core blade 3/19,3/26, 6/70	
Recovery: Auto Tuning/Manual Tuning	

Defects Fixed in Release: v7.2.0d_cvr_brcd_491687_01

Defect ID: DEFECT000491687	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0b	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Tunnel failures due to [BLS-5032], ERROR, WRO_DCX01_BLUE, SLOT 1 DP 2 Soft Faults due to SE Core Panic.	
Condition: FCIP Processing of ELS-PRLI frames received on non-emulating tunnels resets all FCIP objects for that SID/DID pair. In this case, the customer application uses ELS-PRLI frames as a heartbeat/health check frame during active I/O. This leads to error conditions in FCIP data frame processing that is concurrently occurring. This has been in the original design of 7800/FX8-24 FCIP support.	

Defect ID: DEFECT000496527	
Technical Severity: High	**Probability:** High
Product: FOS	**Technology:** Distance
Reported In Release: FOS7.2.0b	**Technology Area:** FCIP
Closed In Release(s): FOS7.2.0d1 (Fixed)	
Symptom: Unable to run traffic on low bandwidth FCIP tunnel. Customer sees application suspends.	
Condition: This may be encountered on low bandwidth FCIP tunnels	