Brocade FOS v7.1.0cb (11) Internal Content Notes

The Brocade CCE process has been used to provide stable code fixes to various Brocade customer sites. This CCE release has been created especially for FCIP FICON Emulation customers that require at a minimum the IBM FICON qualified FOS V7.1.0c code base with important fixes. The base of the CCE release is the IBM FICON Qualified FOS release of V7.1.0c plus confirmed changes.

The current CCE release label is: v7.1.0cb.

The following sections define the defects and improvements that have been added in various builds of the CCE package. CCE packages are available to customer sites through an SR Request to Brocade Support.

CCE releases 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 FOS level.

Note: This document can be shared with customers and partners as required. The following sections include the list of Defects that have been incorporated into the CCE branch and a description of the issue that was addressed.

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
```

FOS v7.1.0cb (11) – 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). These vulnerabilities allow certain malformed function definition to bypass privilege boundaries and execute unauthorized commands.		
Condition:	To exploit these vulnerabilities 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.

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: DEFECT00 527848	**Technical Severity: High**
Summary: FCIP FICON emulation - VM SPOOL DUMP Backup jobs fail after FOS upgrade	
Symptom: VM SPOOL DUMP FICON emulated Tape backup jobs fail after FOS upgrade	
Conditions: After upgrading FOS levels and using FICON Tape Emulation for VM tape operations.	

Defect ID: DEFECT00 526447	Technical Severity: High
Summary: FCIP DP complex stuck in FC RX Flow Control	
Symptom: FX8-24 or 7800 FCIP DP complex Slow FCIP throughput	
Conditions: Multiple very active FCIP Tunnels on a 7800 or FX8-24 FCIP DP complex	
Workaround: None, but can be recovered by a slot power cycle or reset chassis	

FOS v7.1.0ca (10) – Completed on 08/08/2014

Defect ID: DEFECT00 523193	Technical Severity: Medium
Summary: FCIP tape read emulation - ErrorCode=86 during REPOSITION_PENDING_STATE and device busy	
Symptom: IFCC during tape reads.	
Conditions: When FICON tape read pipelining is active and the device presents Device Busy status.	

FOS v7.1.0c9 – Completed on 07/16/2014

Defect ID: DEFECT00 519655	Technical Severity: Medium
Summary: 7800 TX ge ports statistics not showing accurately. portstatsshow gex command	
Symptom: 7800 portstatsshow ge0-5 counters show inaccurate TX packet counts	
Conditions: Port stats output for ge1-5 show no TX packet type stats – ge0 output is summary for all ge0-ge5	

Defect ID: DEFECT00 516703	Technical Severity: High
Summary: FICN-1062 and FICN-1063 abort messages on XRC and IFCC on host	
Symptom: FICN-1062 and FICN-1063 abort messages on XRC and IFCC on host	
Conditions: In a large FICON disk mirroring configuration that includes base and alias devices in the connected primary controllers	
Workaround: None required – IFCCs will occur and normal channel error recovery will complete	

Defect ID: DEFECT00 512507	Technical Severity: High
Summary: FX8-24 Blade limited bandwidth when configured with 2 equal bandwidth tunnels above 7 gig	
Symptom: Customer unable to run above 600 MBs/sec bandwidth on each of two 10G FCIP tunnels	
Conditions: In a dual FCIP path configuration (both DP1 and DP2 are used) with an even number of ingress ports utilizing the FCIP tunnels.	

FOS v7.1.0c8 – Completed on 03/21/2014

FOS v7.1.0c8 includes a merge of CVR v7.1.0c_CVR_445814_5. FOS v7.1.0c_CVR_445814_5 readme is appended at the end of this README. Additional defects are documented as:

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, 7.2.1	
Symptom: CP's paniced during switchshow/supportsave when logical port was in an incomplete state. Standby CP set to faulty continuously even after failover. Switch rebooted.	
Condition: On a rare condition, in a VF environment, if a port is not indexed correctly, subsequent data collection will result in a panic.	
Workaround: When logical ports are found in an inconsistent state, run the command: lfcfg -lislenable Examples of inconsistent states are: "Create Request Sent" "Peer Request Received". This may prevent the switch panic.	

Defect ID: DEFECT000361971	Technical Severity: High
Summary: i2c port reset on Brocade 8G SFPs	
Symptom: **F-Port was logged out of switch due to laser fault during to media access.**	

Defect ID: DEFECT000438017	Technical Severity: High
Summary: SNMP configuration replication overwrites AAA LDAP Settings.	
Symptom: **When trying to replicate SNMP settings alone from one switch to another switch a using BNA or CLI, AAA settings also getting replaced.**	

Defect ID:	DEFECT000452610		
Technical Severity:	High	**Probability:**	Low
Product:	FOS	**Technology:**	Monitoring/RAS
Reported In Release:	FOS7.2.0	**TechnologyArea:**	Bottleneck Detection
Closed In Release(s):	FOS7.1.2, FOS 7.2.0		
Symptom:	Switch set to faulty after a series of detected termination of trafd crashes.		
Condition:	Frequently reboot of switch caused race condition between port offline SCN and getting congestion counters for trunk ports to happen at same time.		
Recovery:	Switch reboot recovers		

Defect ID:	DEFECT000454580		
Technical Severity:	High	**Probability:**	Low
Product:	FOS	**Technology:**	Security
Reported In Release:	FOS6.4.2	**Technology Area:**	Fabric Authentication
Closed In Release(s):	FOS7.1.2, FOS7.2.1		
Symptom:	With SSL configured on Active CP, a newly inserted Standby CP may panic and go through an unnecessary additional reboot.		
Condition:	When SSL is configured on the active CP, inserting a new standby CP with its time set later than that on Active CP & SSL is not already configured, then it may cause a panic & unnecessary additional reboot of standby CP after insertion.		
Workaround:	Do hadisable before inserting standby CP. Then 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: DEFECT000457972	**Technical Severity: High**
Summary:	After an FCIP circuit bounce, invalid buffers index messages are reported on the console.
Symptom:	**After an FCIP tunnel bounces due to a network issue, error messages are generated on console and the TCP connections making up the tunnel/circuit aborts instead of closing gracefully**

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.**	

Defect ID: DEFECT000469915	Technical Severity: High
Summary: nscamshow report state is unknown for remote switches	
Symptom: **nsshowall fails to display PIDS for switches that are connected using long distance E_Ports.**	

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):	Various		
Symptom:	CRC with Good EOF Errors detected which may result in credit loss		
Condition:	This defect updated Serdes value for ICL port for DCX-4s+ In addition, also pulled in tuning in following platforms DCX-4S FC8-48 Slot 1 port 2 1/2 (Defect408703) DCX-4S FC8-48 Slot 2 port 0 and 8; 2/0, 2/8 (Defect 490548) DCX+ FC8-64 Slot 1 port 114, Slot 10 port 154, slot 11 port 154, 1/114, 10/154, 11/154 (Defect452033) Slot 7 port 155, 76, Slot2 port 154 (Defect 492704)		

Defect ID:	DEFECT000481951		
Technical Severity:	High	**Probability:**	Low
Product:	FOS	**Technology:**	Traffic Management
Reported In Release:	FOS7.2.1	**Technology Area:**	FC-FC routing
Closed In Release(s):	FOS7.1.2, FOS7.2.0		
Symptom:	Encountered IO errors when decommissioning an ISL		
Condition:	On 8G switch, in VF environment, If an E_port uses logical port 14 and there are other E_ports to the same domain, and when all other E_ports except logical port 14 are decommissioned, logical port 14 traffic is disrupted.		

Defect ID:	DEFECT000484327		
Technical Severity:	High	**Probability:**	Low
Product:	FOS	**Technology:**	Traffic Management
Reported In Release:	FOS 7.1.0	**Technology Area:**	FC-FC routing
Closed In Release(s):	FOS7.1.2		
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:	Either there is physically duplicated WWPN in the environment, or an interleave offline and online sequence between two different NPIV ports can triggered a false duplicate WWPN detection		
Workaround:	Remove physically duplicate WWPN devices if any exists.		
Recovery:	If there is no physically duplicate WWPN devices, switch recovers itself after panic		

Defect ID: DEFECT000484414	**Technical Severity: High**
Summary: AGshow shows stale entry	
Symptom: **After the AG was removed from the fabric, the AG still remains as a stale entry in agshow comman**	

Defect ID: DEFECT000495636	**Technical Severity: High**
Summary: Lost ASIC data structures results in verify/panic while replacing CP	
Symptom: **Switch Panic during CP replacement**	

Defect ID: DEFECT000461485	Technical Severity: Medium
Summary: FCIP FICON Emulating Tunnel with VTS devices do not recover after the controller has exited service mode	
Symptom: **When a VTS was placed into service mode and then restored to normal mode, not all paths were recovered.**	

Defect ID: DEFECT000470487	Technical Severity: Medium
Summary: Fabric watch not calculating VEX port packet loss correctly.	
Symptom: **Erroneous FW-1190 error messages seen on different VEX tunnels: Event: , VEXport#3/16,Packet Loss, is above high boundary(High=100, Low=0). Current value is 1176 Percentage(%). Severity: Warning**	

Defect ID: DEFECT000477188	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.1	**Technology Area :** Platform Service
Closed In Release(s): FOS7.1.2, FOS7.2.1	
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.	

FOS v7.1.0c7 – Completed on 02/19/2014

Defect ID: **DEFECT00477596**	Technical Severity: Medium
Summary: Chassis is not ready for management state in weblinker due to double termination of weblinker in 3 sec.	
Symptom: Weblinker terminated and restarted but could not service the HTTP requests. All requests getting a response “Chassis is not ready for management”.	
Workaround: Use hafailover or reboot CLI.	

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: DEFECT00465498	Technical Severity: Medium
Summary: Add voltage monitor to FX8-24.	
Symptom: FX8-24 faulted without any trace.	

Defect ID: DEFECT00460296	Technical Severity: Medium
Summary: Unit check during tape repositioning resulted in FICN-1056 FICON Emulation Error code 100	
Symptom: Unit check during tape repositioning resulted in FICN-1056 FICON Emulation Error code 100 and ficon abort.	
Workaround: Disable FICON Tape Read Pipelining on the FCIP Tunnel	

Defect ID: DEFECT00454312	Technical Severity: Medium
Summary: CP panic during taken over as active CP due to access media on a disabled blade	
Symptom: Switch cold boot when there is connection problem between FX8-18 port blade and chassis backend.	
Workaround: None	

FOS v7.1.0c6 – Completed on 01/29/2014

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

Defect ID: DEFECT00490533	Technical Severity: High
Summary: FDR (Fast Dump Restore) zHPF mode job failing when I/Os include a large number of frames in a FC sequence.	
Symptom: zHPF mode job failures and Aborts recorded in the switch RASLOG for FICON devices	
Work around: None	

Defect ID: DEFECT00483044	Technical Severity: Medium
Summary: Add additional debug logic to capture LTO Trap check status.	
Symptom: Intermittent ANR8302E errors on IBM LTO5 library volumes.	
Work around: Disable FCIP Open Systems Tape Read and Write Pipelining.	
Changes added: This version adds FTRACE triggers whenever OSTP accelerated write sequences are dropped due to the receipt of a PLOGI for a tape device.	

FOS v7.1.0c5 – Completed on 11/07/2013

Defect ID: DEFECT00483044	Technical Severity: Medium
Summary: Add additional debug logic to capture LTO Trap check status.	
Symptom: **Unknown**	
Work around: Unknown	

Defect ID: DEFECT00479882	Technical Severity: High
Summary: FICON B7800 XRC Emulation Aborts after Device Level Exception frame is received	
Symptom: **MVS reported IFCCs due to aborted FICON RRS/Device Level Exception/LACK Sequence**	
Work around: Disable FCIP FICON XRC Emulation on the tunnel.	

FOS v7.1.0c4 – Completed on 10/15/2013

Defect ID: DEFECT00477834	Technical Severity: Medium
Summary: ANR8302E errors on IBM LTO5 library	
Symptom: Intermittent ANR8302E errors on IBM LTO5 library volumes.	
Work around: Disable FCIP Open Systems Tape Read and Write Pipelining.	

Defect ID: **DEFECT00474833**	Technical Severity: **Medium**
Summary: FCIP FW Tape Device presenting extra check condition when prior FW sequence ended with check condition.	
Symptom: Job failures after check condition from tape device (the next I/O is incorrectly responded to with a deferred error check condition status).	
Work around: Disable FCIP Fast Write on the tunnel	

FOS v7.1.0c3 – Completed on 09/13/2013

Defect ID: **DEFECT00474234**	Technical Severity: **Medium**
Summary: Multiple Aborted FICON Sequences after processing Emulated Attention in zOS GM configuration	
Symptom: FICN-1062 and FICN-1063 RASLOG messages and associated XTUN-1999 FTRACE messages and zOS IOS000 errors recorded in SYSLOG	
Work around: Disable the FOS v7.1.0c new FCIP FICON emulation Idle Status Accept feature. The feature can be disabled via the following command: `portcfg fciptunnel <slot/>vePort modify --ficon-debug NewFlags` Where `NewFlags` includes the `0x1000` bit.	

Defect ID: **DEFECT00471823**	Technical Severity: **High**
Summary: FICON Tape Write Emulation control variables go negative causing limited tape performance.	
Symptom: Write Emulation Counters go negative causing limited performance. FICON Tape window sizes are never increased from a pipeline of 1 (1 chain). In this case, the customer had multiple 7800 pairs and could see the performance difference when tape jobs were ran through one pair verses a different pair.	
Work around: Reboot the 7800 or FX8-24 blade to reset the control variables for FICON Write Pipelining	

Defect ID: **DEFECT00472886**	Technical Severity: **High**
Summary: FCIP FICON Tape Emulation not getting into Read pipelining due to Synchronizing status bit set in 1st command in chain	
Symptom: Slow FICON Tape Read Performance (long running restore/recall) jobs	
Work around: Change z/OS job characteristics or parameters	

Defect ID: **DEFECT00463747**	Technical Severity: High
Summary: I/O Stops if ISL port disabled in a topology that includes FCIP Tape Pipelining.	
Symptom: I/O stops after ISL ports between edge switch and 7800 are disabled in a topology that includes FCIP Tape Pipelining. Happens when second to last path was disabled and would not failover properly	
Work around: None	

Defect ID: **DEFECT00468795**	Technical Severity: High
Summary: FCIP FICON XRC Emulation Abort after Selective Reset Errors	
Symptom: If FICON XRC Emulation receives a Selective Reset for a device that is currently in Stacked Status State, the Selective Reset is incorrectly responded to by emulation processing leading to an abort sequence from the channel for the Selective Reset Exchange.	
Work around: None	

Defect ID: **DEFECT00450420**	Technical Severity: Medium
Summary: When multiple priorities are run with TPERF with low rate, TPERF timeout.	
Symptom: TPERF terminates when running with all three (-high -medium -low) QOS setting and low bandwidth under 70 Megabits	
Work around: None	

FOS v7.1.0c2 – Completed on 07/17/2013

Defect ID: **DEFECT00460768/465730**	Technical Severity: High
Summary: Blade fault unnecessarily on rare parity errors.	
Symptom: Customer experienced frequent blade fault upon detecting transient self-correctable ASIC errors	
Work around: None	

FOS v7.1.0c1 – Completed on 04/30/2013

Defect ID: **DEFECT00454148**	**Technical Severity: High**
Summary: FCIP FICON OEM Test: Attention status is not being sent to channel	
Symptom: Tape mounts are not always completed.	
Work around: Disable FCIP FICON Tape Read and Write Pipelining or disable the FOS v7.1.0c new FCIP FICON emulation Idle Status Accept feature.	

Defect ID: **DEFECT00 454150**	**Technical Severity: High**
Summary: FCIP FICON OEM Test: Sync Sort job fails sorting 1G random data file	
Symptom: Job receives SIM error and fails	
Work around: Disable the FOS v7.1.0c new FCIP FICON emulation Idle Status Accept feature. The feature can be disabled via the following command: `portcfg fciptunnel <slot/>vePort modify --ficon-debug NewFlags` Where `NewFlags` includes the `0x1000` bit.	

Defect ID: **DEFECT00455673**	**Technical Severity: Medium**
Summary: FCIP FICON Emulated Tape Cancel Aborts and Selective Resets	
Symptom: IFCCs recorded on the connected FICON Channel MVS systems after a tape job was cancelled.	
Work around: Disable FCIP FICON Emulation features on the tunnel.	

Defect ID: **DEFECT00456643**	**Technical Severity: High**
Summary: BLS-5024 event results in loss of configured IPIF info on FCIP Tunnel with IP Sec enabled	
Symptom: With IP Sec enabled FCIP Tunnel after CP HA Failover, BLS-5024 error and then portshow ipif <slot/>/gePort results in "No IP Interfaces found"	
Work around: slotpoweroff/on the impacted FX8-24 slot.	

Defect ID: **DEFECT00453924**	**Technical Severity: High**
Summary: FX8-24 BLS-5024 event results in loss of IPIFs on that blade's 10 GigE port(s)	
Symptom: BLS-5024 event and then one of the 10 gigE ports will not show configured IPIFs and potentially an FCIP Tunnel will not recover.	
Work around: slotpoweroff/on the impacted FX8-24 slot.	

APPENDEX: Brocade CVR 445814 Internal Content Notes

Brocade CVR 445814 Internal Content Notes

The Brocade CVR process has been used to provide stable code fixes to various Brocade customer sites. This CVR has been created especially for FICON Emulation customers that require at a minimum the IBM FICON qualified FOS V7.1.0c code base with important fixes. The base of the CVR is the IBM FICON Qualified FOS release of V7.1.0c plus confirmed changes.

The current CVR label is: v7.1.0c_cvr_brcd_445814_05.

The following sections define the defects and improvements that have been added in various builds of the CVR. CVR Builds are available to customer sites through an SR Request to Brocade Support.

CVRs 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 CVR. As of 2/28/2014, the following TRs fixes are in the following releases:

Release:	**TRs:**
FOS 7.2.0	454148, 454150, 455673, 456643, 453924, 454123, 445814
FOS7.1.1	454123, 445814, 446858, 429815, 443541
FOS7.1.1a	(460768 via 465730), 459831, 471333, 452801, 470123
FOS7.1.1b	457413
Currently not yet fixed in any FOS Release	482106,482736,486638,492854

This document can be shared with customers and partners as required. The following sections include the list of Defects that have been incorporated into the CVR branch and a description of the issue that was addressed.

v7.1.0c_cvr_brcd_445814_05 completed on 2/28/2014

Defect ID:	DEFECT000492854	
Technical Severity:	High	**Probability:** Low
Product:	FOS	**Technology:** Traffic Management
Reported In Release:	FOS7.1.0	**Technology Area:** FC-FC routing
Closed In Release(s):		
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.	

v7.1.0c_cvr_brcd_445814_04 completed on 12/13/2013

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: DEFECT00482736	**Technical Severity: High**
Summary: FICON CUP sending continuous unsolicited alerts to host reporting a FRU failure.	
Symptom: Enabling FMS mode leads to floods of internal FICU raslog after code upgrade when there are 10 or more outstanding Fru failures messages.	
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	

v7.1.0c_cvr_brcd_445814_03 completed on 10/23/2013

Defect ID: **DEFECT00457413**	**Technical Severity: High**
Summary: ICL ports having lots of credit loss after hafailover causing them to port_flt	
Symptom: All ICL ports go to In_Sync and port_flt	
Workaround: None	

v7.1.0c_cvr_brcd_445814_02 completed on 9/6/2013

Defect ID: **DEFECT00471333**	**Technical Severity: Critical**
Summary: Incoming corrupted Flogi frame triggered switch to panic in a Loop.	
Symptom: Switch starts rolling reboot. After it stops, type in any command, it will show: "fabos not yet initialized". Further investigation shows device FLogi has certain Vendor Version Level (VVL) bits set unexpectedly	
Workaround: Keep the port connected to the misbehaving device in disabled state	

Defect ID: **DEFECT00429815**	**Technical Severity: High**
Summary: Switch exhibits snmpd crash and switch reboot when being managed by BNA.	
Symptom: Switches running in AG mode and managed by BNA exhibit snmpd crash and switch reboot	
Workaround: Avoid managing an AG switch with BNA or have all ports connected to either N_Port or F_port or have AG in auto policy disabled state.	

Defect ID: **DEFECT00443541**	**Technical Severity: Medium**
Summary: Continuous FSS-1001 messages are seen after firmware upgrade from FOS v6.4.2a to v6.4.3c	
Symptom: Continuous FSS-1001 messages after firmware upgrade due to inconsistent Access Gateway State Synchronization	
Workaround: None.	

Defect ID: DEFECT00470123	Technical Severity: High
Summary: Switch running agshow panics or BNA seed switch panics when polling for AG info in a fabric with AG switches.	
Symptom: After the port connecting AG to switch bounces, before fabric management server and name server data base are stabilized, polling from BNA caused seed switch to panic, similarly run agshow on switch can cause switch to panic. The timing window for triggering the panic is very small.	
Workaround: Avoid agshow CLI and managing switch via BNA.	

Defect ID: DEFECT00 446858	Technical Severity: Medium
Summary: In a heavily congested fabric, if a HAfailover happens when a backend port is reporting frame timeout, switch falsely identifies stuck VC and performs link reset.	
Symptom: Switch continuously reports RASLOG "C2-1014, Link Reset" on backend port, and under rare occasion, observed switch panic	
Workaround: None.	

Defect ID: DEFECT00452801	Technical Severity: Medium
Summary: Switch unable to process commands	
Symptom: The Switch becomes unmanageable and will not accept FOS commands, including 'Reboot'. The only way to recover is to power cycle the switch.	
Workaround: Avoid querying invalid class from WT.	

v7.1.0c_cvr_brcd_445814_02 also including following defect that was part of 7.1.0C2 CEE release:

Defect ID: DEFECT00460768	Technical Severity: High
Summary: Blade fault unnecessarily on rare parity errors	
Symptom: Customer experienced frequent blade fault upon detecting transient self-correctable ASIC errors	
Workaround: None.	

v7.1.0c_cvr_brcd_445814_01 completed on 5/24/2013

Defect ID: **DEFECT00445814**	Technical Severity: Medium
Summary: Configuration download failure when downloading fabric watch settings	
Symptom: After configure download from CLI or use BNA to do partial fabric watch data replication, Bottleneck configurations were removing from the switch.	
Workaround: None.	

Defect ID: DEFECT00454123	Technical Severity: High
Summary: Unable to launch EZManager.	
Symptom: EZManager status bar stops at 53% and throws an exception halting the launch	
Workaround: None	

v7.1.0c_cvr_brcd_445814_01 also including following defect that was part of 7.1.0C1 CEE release:

Defect ID: **DEFECT00454148**	Technical Severity: High
Summary: FCIP FICON OEM Test: Attention status is not being sent to channel	
Symptom: Tape mounts are not always completed..	
Workaround: Disable FCIP FICON Tape Read and Write Pipelining or disable the FOS v7.1.0c new FCIP FICON emulation Idle Status Accept feature.	

Defect ID: DEFECT00454150	Technical Severity: High
Summary: FCIP FICON OEM Test: Sync Sort job fails sorting 1G random data file	
Symptom: Job receives SIM error and fails	
Workaround: Disable the FOS v7.1.0c new FCIP FICON emulation Idle Status Accept feature. The feature can be disabled via the following command: portcfg fciptunnel <slot/>vePort modify –ficon-debug NewFlags Where NewFlags includes the 0x1000 bit.	

Defect ID: **DEFECT00455673**	**Technical Severity: Medium**
Summary: FCIP FICON Emulated Tape Cancel Aborts and Selective Resets	
Symptom: **IFCCs recorded on the connected FICON Channel MVS systems after a tape job was cancelled.**	
Workaround: Disable FCIP FICON Emulation features on the tunnel.	

Defect ID: **DEFECT00456643**	**Technical Severity: High**
Summary: BLS-5024 event results in loss of configured IPIF info on FCIP Tunnel with IP Sec enabled	
Symptom: **With IP Sec enabled FCIP Tunnel after CP HA Failover, BLS-5024 error and then portshow ipif <slot/>/gePort results in "No IP Interfaces found"**	
Work around: slotpoweroff/on the impacted FX8-24 slot.	

Defect ID: **DEFECT00453924**	**Technical Severity: High**
Summary: FX8-24 BLS-5024 event results in loss of IPIFs on that blade's 10 GigE port(s)	
Symptom: **BLS-5024 event and then one of the 10 gigE ports will not show configured IPIFs and potentially an FCIP Tunnel will not recover.**	
Work around: slotpoweroff/on the impacted FX8-24 slot.	