Brocade v7.0.0d1 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 Emulation customers that require at a minimum the IBM FICON qualified FOS V7.0.0d code base with important fixes. The base of the CCE is the IBM FICON Qualified FOS release of V7.0.0d plus confirmed changes.

The current CCE label is: v7.0.0d1.

The following sections define the defects and improvements that have been added in various builds of the CCE. 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. As of 10/09/2014, the following TRs fixes are in the following releases:

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 v7.0.0d1 is equivalent to FOS CVR 419235 Build 9 – 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, FOS7.0.0d1, 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: DEFECT00505359	**Technical Severity: Medium**
Summary: Switch panics intermittently after SS command is started	
Symptom: Switch panic during supportsave.	
Workaround: Contact support to remove RTE section data gathering from supportsave	

Defect ID: **DEFECT00383558**	Technical Severity: **Medium**
Summary: Director with FX8-24 occasionally panics when performing a supportsave when switch is configured in FMS mode	
Symptom: **Switch panic during supportsave.**	
Workaround: Contact support to remove RTE section data gathering from supportsave	

Defect ID: **DEFECT00389303**	Technical Severity: **High**
Summary: Switch finds inconsistency in domain count and E-port count during HAfailover	
Symptom: After FOS upgrade, multiple ports report "Not ready for F or L ports"	
Workaround: Manual fabric rebuilds by bouncing a downstream/upstream ISL port/trunk. No impact to F port if domain ID does not change during bounce.	

Defect ID: **DEFECT00419235**	Technical Severity: **Medium**
Summary: Devices attached to failing FC10-6 port may report errors.	
Symptom: FOS does not report physical port errors detected on FC10-6 10 Gpbs ports	

Defect ID: **DEFECT00470487**	Technical Severity: **Medium**
Summary: Fabric Watch does 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: **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	

Defect ID: DEFECT00376595	
Summary: Replication of FABRIC WATCH through BNA fails in Brocade switches in VF	
Symptom: **User cannot replicate fabric watch only data through BNA. CLI works if fabic.name is added to configure file; However both CLI and BNA removed bottleneck detection configure data.**	
Workaround: Use CLI	

Defect ID: DEFECT00419235	**Technical Severity: Medium**
Summary: FOS software does not expose 10 Gpbs user port physical errors on a FC10-6 blade	
Symptom: **Need to monitor 10G ASIC internal errors and report to user via raslog EGR-1000 and EGR-1001**	
Workaround: None	
Defect ID: DEFECT00431920	**Technical Severity: High**
Summary: Support the documented BRCD-FCIP-Ext MIB in MIB reference	
Symptom: **User will always see 0 for the below measures** **1. fcipExtendedLinkTcpDroppedPackets** **2. fcipExtendedLinkTcpSmoothedRTT** **3. fcipExtendedLinkRtxRtxTO** **4. fcipExtendedLinkRtxDupAck** **5. fcipExtendedLinkDupAck**	
Workaround: None	
Defect ID: DEFECT00373218	**Technical Severity: High**
Summary: Memory leaks on standby CP during execution of supportsave	
Symptom: **CP panics after multiple interactions of supportsave. Memory block used for "buffer_head" increased significantly**	
Workaround: Reboot standby CP when memory is low	

Defect ID: DEFECT00358156	**Technical Severity: High**
Summary: FCIP Tunnel bounce caused by chip reset. PCIe errors throughout errdumpall	
Symptom: Chip reset due to PCIe errors with raslog BLS-5023. The chip reset can cause tunnel bounce and IO halt	
Work around: Issue is seen **less when ipsec is disabled.**	
Defect ID: DEFECT00358156	**Technical Severity: High**
Summary: FCIP Tunnel bounce caused by chip reset. PCIe errors throughout errdumpall	
Symptom: Chip reset due to PCIe errors with raslog BLS-5023. The chip reset can cause tunnel bounce and IO halt	
Work around: Issue is seen **less when ipsec is disabled.**	

Defect ID: DEFECT00358156	**Technical Severity: High**
Summary: FCIP Tunnel bounce caused by chip reset. PCIe errors throughout errdumpall	
Symptom: Chip reset due to PCIe errors with raslog BLS-5023. The chip reset can cause tunnel bounce and IO halt	
Work around: Issue is seen **less when ipsec is disabled.**	

Defect ID: DEFECT00419620	**Technical Severity: Meidum**
Summary: An hafailover, hareboot or firmwaredownload may cause offline ports with a ASIC register being zeroed out	
Symptom: If frames are queued to the offline ports, credit is permanently lost and observe busy buffer condition on the port	
Work around: None	

Defect ID: DEFECT00403592	**Technical Severity: Meidum**
Summary: Frame discards after enabling new TI zone	
Symptom: After enabling a new TI zone with failover enabled and all member ports disabled, discards due to un-routable were observed in another TI zone	
Work around: None	

Defect ID: DEFECT00415795	**Technical Severity: High**
Summary: DCX with FC10 blade continuous reboots after fwdl; blades stuck in POST2 before chassis reboots	
Symptom: When FC10 blades run POST, DCX went into a continuous reboot loop until POST was disabled	
Work around: Disable diagnostic POST.	
Defect ID: DEFECT00 423389	**Technical Severity: High**
Summary: Switch panic while running suppotsave with 4G blades.	
Symptom: In FOS v7.0.x, When RTE (route module) portion of supportsave is run on 4G blade, it triggered switch panic. This was only reported by one customer site but multiple times.	
Work around: Avoid running supportsave during route change	

Defect ID: DEFECT00386010	**Technical Severity: Medium**
Summary: Device does re-FLOGI with a different WWN cause stale entry in Flogin DataBase	
Symptom: switch reports duplicate WWN and panic.	
Work around: None	

Defect ID: DEFECT00 409878	**Technical Severity: Medium**
Summary: HTTPD (Apache server 1.3.31-10) goes to defunct state	
Symptom: Customer loses manageability via BNA	
Work around: Restart httpd or HAfailover (hareboot)	