Brocade FOS Release v6.4.3f3 Internal Content Notes

The Brocade CCE process has been used to provide stable code fixes to various Brocade customer sites. 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
```

v6.4.3f3 was completed on 10/8/2014

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 can 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.		

v6.4.3f2 was completed on 09/23/2014

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: DEFECT000478895	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.0	**Technology Area:** SNMPv2, SNMPV3 &Mib
Closed In Release(s): FOS7.2.1, FOS7.3.0	
Symptom: snmpd memory usage increases.	
Condition: Switch was poll with SNMPv1 when it is disabled on switch.	
Workaround: Do not poll the switch with SNMPv1 when it is disabled in switch or manage the switch via SNMPv3.	

Defect ID: DEFECT000519293	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS6.4.3	**Technology Area:** Web Tools
Closed In Release(s): FOS7.0.0	
Symptom: HAfailover is triggered by low memory condition.	
Condition: Switch is monitored by webtools or BNA and switch has ports with custom bottleneck settings	

Defect ID: DEFECT000519003	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Distance
Reported In Release: FOS6.4.3	**Technology Area:** FCIP
Closed In Release(s): FOS7.3.0b	

Symptom:	FICON Tape Backup/restore jobs are failing using FICON Emulation enabled tunnels
Condition:	FICON Emulation enabled tunnels on the 7500, FR4-18i, 7800, FX8-24 and 7840s with a new OEM virtual tape controller and micro code.
Workaround:	Disable FICON Acceleration

v6.4.3f1 was completed on 06/09/2014

Defect ID:	DEFECT000503299		
Technical Severity:	High	**Probability:**	Low
Product:	FOS	**Technology:**	Other
Reported In Release:	FOS6.4.3	**Technology Area:**	Other
Closed In Release(s):	FOS7.0.2e, FOS7.2.1b, FOS7.3.0		
Symptom:	After FOS upgrade, CLI "swithchsow" 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.		
Recovery:	Trigger fabric rebuild by executing "fabricprincipal -f". Manual fabric rebuild by taken offline ALL E_port/Trunks, then re-enable them or switch disable/enable.		

Defect ID:	DEFECT000503059		
Technical Severity:	Medium	**Probability:**	Medium
Product:	FOS	**Technology:**	Management
Reported In Release:	FOS6.4.3	**Technology Area:**	Firmware upload/download
Closed In Release(s):			
Symptom:	Downgrading from FOS v6.4.3f to v6.3.0 failed, and customer gets an error "Please use reboot to reboot the switch manually".		
Condition:	The issue happens on v6.4.3f with Brocade300 on downgrade only, it does not apply to FOS v7.3		

Defect ID:	DEFECT000484414		
Technical Severity:	High	**Probability:**	Medium
Product:	FOS	**Technology:**	Virtualization
Reported In Release:	FOS7.0.2	**Technology Area:**	Access Gateway
Closed In Release(s):	FOS7.0.2e ,FOS7.1.2b, FOS7.2.1b, FOS7.3.0		
Symptom:	Under rare conditions, Access Gateway(AG) entries stay in management server (MS) database even after removing them from the fabric. FOS firmware is expected to remove these stale entries during execution of agshow CLI command. However, due to a timing issue the stale entries may not be removed from the database when agshow CLI command is run.		
Condition:	This may be observed on a switch running firmware version higher than v7.0.		

Defect ID: DEFECT000401075	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Security
Reported In Release: FOS7.0.1	**Technology Area:** Fabric Authentication
Closed In Release(s): FOS7.1.c, FOS7.2.1b, FOS7.3.0	
Symptom: Weblinker crashes and cannot be restarted	
Condition: When one of the radius server is not responding for reasons such as port 1813 is blocked by network firewall, then next available server to authenticate the radius user triggers a NULL pointer access.	
Workaround: Unblocking the accounting port (default port 1813) is the workaround in case of accounting fails due to firewall.	