Brocade FOS Release v6.2.2f9 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
```

v6.2.2f9 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 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.		

v6.4.3f8 was completed on 07/24/2014

Defect ID:	DEFECT000500843		
Technical Severity:	High	**Probability:**	Low

Product: FOS	**Technology:** Management
Reported In Release: FOS7.2.2	**Technology Area:** CLI
Closed In Release(s): FOS7.3.0	
Symptom: After hot swapping BR4016 into a server chassis, customer experienced disruptive firmwaredownload.	
Condition: Need to hot swap of the embedded switch, and only impact the first hareboot.	

v6.2.2f7 was completed on 04/17/2014

Defect ID: DEFECT000418392	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS7.1.0	**Technology Area:** Web Tools
Closed In Release(s): FOS6.4.3f, FOS7.0.2e, FOS7.1.0	
Symptom: Weblinker crash while the fabric is being monitored by Brocade Network Advisor.	
Condition: This may be encountered in a large fabric with security policy activated.	

v6.2.2f6 was completed on 09/06/2013

Defect ID: DEFECT000461110	
Technical Severity: Medium	**Probability:** Medium
Product: FOS	**Technology:** Management
Reported In Release: FOS6.2.2	**Technology Area:** Web tool
Closed In Release(s):	
Symptom: Switch panic due to Weblinker causing out of memory condition	
Condition: When the switch in AG mode is managed by BNA continuously	

v6.2.2f5 was completed on 07/23/2013

Defect ID: DEFECT000272365	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Management
Reported In Release: FOS6.2.1	**Technology Area:** Web Tools
Closed In Release(s): FOS	
Symptom: Weblinker restart	
Condition: Qualys security scan causes weblinker restart after getting HTTP_HOST attribute as NULL from request payload.	

v6.2.2f4 was completed on 04/03/2013

Defect ID: DEFECT000429815

Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS6.4.2	**Technology Area:** Access Gateway
Closed In Release(s): FOS6.4.3e, FOS7.0.2d, FOS7.1.1, FOS7.2.0	
Symptom: Switches running in AG mode and managed by BNA exhibit snmpd crash and switch reboot.	
Condition: Switch exhibits snmpd crash and switch reboot when being managed by BNA	
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.	

v6.2.2f3 was completed on 12/10/2012

Defect ID: DEFECT000301448	
Technical Severity: High	**Probability:** Medium
Product: FOS	**Technology:** Other
Reported In Release: FOS6.4.0	**Technology Area:** Other
Closed In Release(s): FOS6.3.2, FOS6.4.0b, FOS7.0.0	
Symptom: Build Fabric sent to Access Gateway with F-Port trunking.	
Condition: When F-Port trunking is activated and after the master trunk goes offline, the switch will add the new master trunk to the list of ports, which will send EFP/BF/DIA flood. The ports will remain in this state until all N-Ports are taken offline and logged back into the fabric again. Build Fabric (BF) sent to AG and AG forwarding the BF to redundant fabric caused fabric disruption.	

v6.2.2f2 was completed on 09/17/2012

Defect ID: DEFECT000407753	
Technical Severity: High	**Probability:** Low
Product: FOS	**Technology:** Virtualization
Reported In Release: FOS6.2.2	**Technology Area:** Access Gateway
Closed In Release(s): FOS7.1.0	
Symptom: AG F_port goes disabled due to N-port busy	
Condition: If there is only one N-port, and the F-port was previously associated with that N-port, then it will stay disabled during FAILOVER or FAILBACK	

v6.2.2f1 was completed on 02/01/2012

Defect ID: DEFECT000314056	
Technical Severity: Medium	**Probability:** Low
Product: FOS	**Technology:** Other
Reported In Release: FOS5.3.0	**Technology Area:** Other
Closed In Release(s): FOS6.2.2d, FOS6.3.2c, FOS6.4.1a, FOS7.0.0, FOS7.0.2	
Symptom: Due to incorrect internal counter logic, PORT-1003 port faults are being reported in the RASLOG when they shouldn't be.	
Condition: After a long switch uptime, if there are greater than 50 link down events before a switch is rebooted	

	(as opposed to within 2 minutes), the port is faulted with a PORT-1003 being reported in the RASLOG.