Brocade FOS Release v6.4.2a3 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 v6.4.2a code base with important fixes. The base of the CCE is the IBM FICON Qualified FOS release of v6.4.2a plus confirmed changes.

The current CCE label is: v6.4.2a3.

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
```

v6.4.2a3 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). 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.

V6.4.2a2 was completed on 10/15/2012

Defect ID:	DEFECT000415165		
Technical Severity:	Medium	**Probability:**	Low
Product:	FOS	**Technology:**	Traffic Management
Reported In Release:	FOS6.4.2	**Technology Area:**	Port Bring Up
Closed In Release(s):	FOS6.4.3c, FOS7.0.2a, FOS7.1.0, FOS7.1.2		
Symptom:	In a mainframe setup, many Nport are bounced at the same time and some hosts cannot see storage.		
Condition:	A fast FLOGI frame comes in before the port state has changed to AC (Active online) caused various switch problems.		

V6.4.2a1 was completed on 02/15/12012

Defect ID:	DEFECT000325716		
Technical Severity:	Medium	**Probability:**	Low
Product:	FOS	**Technology:**	Virtualization
Reported In Release:	FOS7.0.0_bld01	**Technology Area:**	Encryption
Closed In Release(s):	FOS7.0.0		
Symptom:	Unsupported SCSI commands are not rejected and cause server to misbehave (hang).		
Condition:	In environment with servers that are configured to send XCOPY or WRITE SAME SCSI command		
Workaround:	Disable VAAI in server		