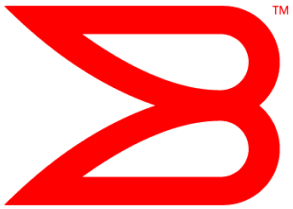

TECH NOTE

Fabric OS Security Vulnerability Report

April 15, 2014

BROCADE

Contents

CVE-1999-0517

Field	Description
Title	An SNMP community name is the default (e.g. public), null, or missing.
CVE ID / Primary Reference	CVE-1999-0517
Other References	CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-1999-0792,CVE-2000-0147, CVE-2001-0380, CVE-2001-0514, CVE-2001-1210, CVE-2002-0109, CVE-2002-0478, CVE-2002-1229, CVE-2004-0311, CVE-2004-1474, CVE-2010-1574
CVSS Score	7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	FOS versions 6.4.x and newer
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	An SNMP community name is the default (e.g. public), null, or missing.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0517
Alert Impact	Impacted – Apply Brocade Remedy
Risk	High
Technical Details	The Brocade product is shipped with default community strings. Best practices dictate that all default community strings be changed during initial configuration.
Brocade Defect Number	
Date of Last Modification	2014-04-15

CVE-2006-3918

Field	Description
Title	httpd: Expect header XSS
CVE ID / Primary Reference	CVE-2006-3918
Other References	CVE-2007-5944
CVSS Score	4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed	Not Applicable

Versions	
OS	Not Applicable
Application	Not Applicable
Summary	http_protocol.c in (1) IBM HTTP Server 6.0 before 6.0.2.13 and 6.1 before 6.1.0.1, and (2) Apache HTTP Server 1.3 before 1.3.35, 2.0 before 2.0.58, and 2.2 before 2.2.2, does not sanitize the Expect header from an HTTP request when it is reflected back in an error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated using a Flash SWF file.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3918
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not support Flash files.
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2008-5161

Field	Description
Title	SSH CBC vulnerability
CVE ID / Primary Reference	CVE-2008-5161
Other References	
CVSS Score	2.6 (LOW) (AV:N/AC:H/AU:N/C:P/I:N/A:N)
Scanning Tool and Version	Nessus Version 5.2.5
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in

	an SSH session via unknown vectors.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not support affected OpenSSH version.
Brocade Defect Number	
Date of Last Modification	2014-04-15

CVE-2010-4478

Field	Description
Title	openssh: J-PAKE authentication bypass
CVE ID / Primary Reference	CVE-2010-4478
Other References	None
CVSS Score	7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4478
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not enable J-PAKE.
Brocade Defect	

Number	
Date of Last Modification	2014-01-23

CVE-2010-5107

Field	Description
Title	OpenSSH Denial of Service Vulnerability
CVE ID / Primary Reference	CVE-2010-5107
Other References	None
CVSS Score	5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Scanning Tool and Version	Nessus, version not identified
Affected Versions	FOS versions 6.4.x and newer
Target Fixed Versions	FOS 7.3.0
OS	Not Applicable
Application	Not Applicable
Summary	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5107
Alert Impact	Remedy in Progress
Risk	Medium
Technical Details	The Brocade product embeds the vulnerable code/component. A patch is targeted for FOS version 7.3.0. Brocade defect number 472221 has been opened to track this issue.
Brocade Defect Number	472221
Date of Last Modification	2014-01-23

CVE-2011-1739

Field	Description
Title	FreeBSD 'mountd' Incorrect Netmask Access Control List (ACL) Security Bypass Vulnerability
CVE ID / Primary Reference	CVE-2011-1739
Other References	None

CVSS Score	4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	The makemask function in mountd.c in mountd in FreeBSD 7.4 through 8.2 does not properly handle a -network field specifying a CIDR block with a prefix length that is not an integer multiple of 8, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances via an NFS mount request.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1739
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not use the FreeBSD kernel.
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2011-3188

Field	**Description**
Title	Modified MD4 algorithm used in IPv4 and IPv6 implementations in the Linux kernel before 3.1 is vulnerable to sequence number guessing
CVE ID / Primary Reference	CVE-2011-3188
Other References	None
CVSS Score	6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	FOS versions 6.4.x and newer
Target Fixed Versions	
OS	Not Applicable
Application	Not Applicable
Summary	The (1) IPv4 and (2) IPv6 implementations in the Linux kernel before 3.1 use a modified MD4 algorithm to generate sequence numbers and Fragment Identification values, which makes it

	easier for remote attackers to cause a denial of service (disrupted networking) or hijack network sessions by predicting these values and sending crafted packets.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3188 https://bugzilla.redhat.com/show_bug.cgi?id=732658
Alert Impact	Remedy in Progress
Risk	Medium
Technical Details	The Brocade product embeds the vulnerable code/component. A patch is targeted for FOS version 7.3.0. Brocade defect number 435054 has been opened to track this issue.
Brocade Defect Number	435054
Date of Last Modification	2013-10-01

CVE-2011-3192

Field	Description
Title	httpd: multiple ranges DoS
CVE ID / Primary Reference	CVE-2011-3192
Other References	None
CVSS Score	7.8 (HIGH) (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Scanning Tool and Version	Not identified
Affected Versions	FOS 6.4.x, 7.0.0x, 7.0.1x
Target Fixed Versions	FOS 7.0.2, 7.1.0
OS	Not Applicable
Application	Not Applicable
Summary	The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192
Alert Impact	Impacted – Apply Brocade Remedy
Risk	Medium
Technical Details	The Brocade product embeds the vulnerable code/component. A countermeasure has been tested and verified in the Target Fixed Versions identified above.
Brocade Defect	374751

Number	
Date of Last Modification	2014-01-23

CVE-2011-3368

Field	Description
Title	httpd: reverse web proxy vulnerability
CVE ID / Primary Reference	CVE-2011-3368
Other References	None
CVSS Score	5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not use the mod_proxy module.
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2011-3389

Field	Description
Title	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft

	Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
CVE ID / Primary Reference	CVE-2011-3389
Other References	None
CVSS Score	4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:N/A:N)
Scanning Tool and Version	Not identified
Affected Versions	FOS 6.4.x, 7.0.x, 7.1.0x, 7.1.1, 7.1.1a, 7.2.0
Target Fixed Versions	FOS 7.1.1b, 7.1.2, 7.2.0a, 7.2.1
OS	Not Applicable
Application	Not Applicable
Summary	The HTTPS protocol is vulnerable to attack based on knowledge of the IVs used for CBC ciphers in SSL 3.0/TLS 1.0 implemented in OpenSSL.
Link to advisories	http://www.openssl.org/~bodo/tls-cbc.txt http://cvs.openssl.org/chngview?cn=6452
Alert Impact	Impacted – Apply Brocade Remedy
Risk	Low
Technical Details	The Brocade product embeds the vulnerable code/component. A countermeasure has been tested and verified in the Target Fixed Versions identified above.
Brocade Defect Number	466777
Date of Last Modification	2014-01-23

CVE-2011-3607

Field	**Description**
Title	httpd: ap_pregsub Integer overflow to buffer overflow
CVE ID / Primary Reference	CVE-2011-3607
Other References	None

CVSS Score	4.4 (MEDIUM) (AV:L/AC:M/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607
Alert Impact	Not Exploitable
Risk	Low
Technical Details	The flaw exists but it is not exploitable. The exploit requires local, privileged access to first manipulate the switch. The vulnerability, which results in a resource exhaustion condition, is not regarded as a security issue. Please refer to the following links for more information: https://bugzilla.redhat.com/show_bug.cgi?id=750935 http://thread.gmane.org/gmane.comp.apache.devel/46339/focus=46768
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2012-0021

Field	**Description**
Title	httpd: NULL pointer dereference crash in mod_log_config
CVE ID / Primary Reference	CVE-2012-0021
Other References	None
CVSS Score	2.6 (LOW) (AV:N/AC:H/Au:N/C:N/I:N/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed	Not Applicable

Versions	
OS	Not Applicable
Application	Not Applicable
Summary	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server 2.2.17 through 2.2.21, when a threaded MPM is used, does not properly handle a %{}C format string, which allows remote attackers to cause a denial of service (daemon crash) via a cookie that lacks both a name and a value.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0021
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS versions through 7.1.x use Apache version 2.0.50, which does not contain this vulnerability.
Brocade Defect Number	
Date of Last Modification	2013-08-14

CVE-2012-0027

Field	**Description**
Title	The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher.
CVE ID / Primary Reference	CVE-2012-0027
Other References	None
CVSS Score	5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0027
Alert Impact	Not Exploitable

Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not support GOST.
Brocade Defect Number	
Date of Last Modification	2013-08-14

CVE-2012-0031

Field	Description
Title	scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.
CVE ID / Primary Reference	CVE-2012-0031
Other References	None
CVSS Score	4.6 (MEDIUM) (AV:L/AC:L/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	Apache webservers may use a shared memory segment to share child process status information (scoreboard) between the child processes and the parent process running as root. A child running with lower privileges(such as a PHP or CGI script) than the parent process might trigger an invalid free in the privileged parent process during parent shutdown by modifying data on the shared memory segment.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031
Alert Impact	Not Exploitable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not utilize the scoreboard.c module.
Brocade Defect Number	
Date of Last	2013-08-14

Modification	

CVE-2012-0050

Field	Description
Title	OpenSSL 0.9.8s and 1.0.0f does not properly support DTLS applications, which allows remote attackers to cause a denial of service (crash) via unspecified vectors related to an out-of-bounds read.
CVE ID / Primary Reference	CVE-2012-0050
Other References	None
CVSS Score	5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	OpenSSL 0.9.8s and 1.0.0f does not properly support DTLS applications, which allows remote attackers to cause a denial of service (crash) via unspecified vectors related to an out-of-bounds read. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-4108.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0050
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS versions through 7.2.x use OpenSSL version 0.9.8d, which does not contain this vulnerability.
Brocade Defect Number	
Date of Last Modification	2014-04-15

CVE-2012-0053

Field	Description
Title	httpd: cookie exposure due to error responses
CVE ID /	CVE-2012-0053

Primary Reference	
Other References	None
CVSS Score	4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:N/A:N)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	Title Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS versions through 7.2.x use Apache version 2.0.50, which does not contain this vulnerability.
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2012-0883

Field	**Description**
Title	httpd: insecure handling of LD_LIBRARY_PATH in envvars
CVE ID / Primary Reference	CVE-2012-0883
Other References	None
CVSS Score	6.9 (MEDIUM) (AV:L/AC:M/Au:N/C:C/I:C/A:C)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed	Not Applicable

Versions	
OS	Not Applicable
Application	Not Applicable
Summary	envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not support "apachectl" commands.
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2012-0884

Field	Description
Title	A weakness in the OpenSSL CMS and PKCS #7 code can be exploited using Bleichenbacher's attack on PKCS #1 v1.5 RSA padding also known as the million message attack (MMA).
CVE ID / Primary Reference	CVE-2012-0884
Other References	None
CVSS Score	5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0884

Alert Impact	Not Exploitable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not utilize CMS or PKCS #7.
Brocade Defect Number	
Date of Last Modification	2013-08-14

CVE-2012-2110

Field	Description
Title	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.
CVE ID / Primary Reference	CVE-2012-2110
Other References	None
CVSS Score	7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2110
Alert Impact	Not Exploitable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not use the asn1_d2i_read_bio function.
Brocade Defect	

Number	
Date of Last Modification	2013-08-14

CVE-2012-2131

Field	Description
Title	Multiple integer signedness errors in crypto/buffer/buffer.c in OpenSSL 0.9.8v allow remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-2110.
CVE ID / Primary Reference	CVE-2012-2131
Other References	None
CVSS Score	7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	Multiple integer signedness errors in crypto/buffer/buffer.c in OpenSSL 0.9.8v allow remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-2110.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2131
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS versions through 7.2.x use OpenSSL version 0.9.8d, which does not contain this vulnerability.
Brocade Defect Number	
Date of Last Modification	2014-04-15

CVE-2012-2333

Field	Description
Title	A flaw in the OpenSSL handling of CBC mode ciphersuites in TLS 1.1, 1.2 and DTLS can be exploited in a denial of service attack on both clients and servers
CVE ID / Primary Reference	CVE-2012-2333
Other References	None
CVSS Score	6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2333
Alert Impact	Not Exploitable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not support TLS 1.1.
Brocade Defect Number	
Date of Last Modification	2013-08-14

CVE-2012-2687

Field	Description
Title	httpd: mod_negotiation XSS via untrusted file names in directories with MultiViews enabled
CVE ID / Primary Reference	CVE-2012-2687
Other	None

References	
CVSS Score	2.6 (LOW) (AV:N/AC:H/Au:N/C:N/I:P/A:N)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687
Alert Impact	Not Applicable
Risk	Low
Technical Details	This Cross-site scripting (XSS) vulnerability occurs when the web application dynamically generates different web pages that contain attackers' untrusted data/malicious script. This script will enter into the back end and attack the system while executing it. FOS accepts only requests containing known fixed files so is not exposed to this vulnerability.
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2013-5211

Field	**Description**
Title	ntp: DoS in monlist feature in ntpd
CVE ID / Primary Reference	CVE-2013-5211
Other References	VU#348126
CVSS Score	5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable

OS	Not Applicable
Application	Not Applicable
Summary	The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests, as exploited in the wild in December 2013.
Link to advisories	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5211
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not run the NTPd daemon.
Brocade Defect Number	
Date of Last Modification	2014-01-23

CVE-2014-0160

Field	Description
Title	The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
CVE ID / Primary Reference	CVE-2014-0160
Other References	None
CVSS Score	5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Scanning Tool and Version	Not identified
Affected Versions	None
Target Fixed Versions	Not Applicable
OS	Not Applicable
Application	Not Applicable
Summary	The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
Link to	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160

advisories	
Alert Impact	Not Applicable
Risk	Low
Technical Details	FOS is not exposed to this vulnerability. FOS does not use any version of OpenSSL that contains this vulnerability.
Brocade Defect Number	
Date of Last Modification	2014-04-09