Brocade Security Advisory ID: BSA-2015-003
Initial Publication Date: April 24, 2015
Revision: 7.0
Revision Date: March 23, 2017

Component: OpenSSL
CVSS: 5.0

CVE-2014-3569: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3569

The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.2.1.R5.
Brocade Fabric OS	Not impacted
Brocade Network OS	Not impacted
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release. Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted - Users of the Services Controller VA version 2.0 should upgrade to a newer version. Users of Services Controller s/w installs should consult their OS vendors to ensure their systems are secure.
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Impacted – Fixed in 4.9-35119 and later, which includes openssl-1.0.1k or newer.
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Brocade Security Advisory ID: BSA-2015-003
Initial Publication Date: April 24, 2015
Revision: 7.0
Revision Date: March 23, 2017

Component: OpenSSL
CVSS: 5.0

CVE-2014-3570: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3570

The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.2.1R5.
Brocade Fabric OS	Impacted – Fixed in 8.0.1.
Brocade Network OS	Impacted – Fixed in 6.0.2.
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Impacted - Fixed in 12.5.02c, ADX 12.5.01J, ADX 12.4.00w, and above.
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release, Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted - Users of Services Controller VAs 2.0 or earlier should upgrade to a newer version of the Services Controller. Users of Services Controller s/w installs should consult their OS vendors to ensure their systems are secure.
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Impacted – Fixed in 4.9-35119 and later.
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Brocade Security Advisory ID: BSA-2015-003
Initial Publication Date: April 24, 2015
Revision: 7.0
Revision Date: March 23, 2017

Component: OpenSSL
CVSS: 5.0

CVE-2014-3571: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3571

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.2.1R5.
Brocade Fabric OS	Not impacted
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release, Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted - Users of Services Controller VAs 2.0 or earlier should upgrade to a newer version of the Services Controller. Users of Services Controller s/w installs should consult their OS vendors to ensure their systems are secure.
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Impacted – Fixed in 4.9-35119 and later releases.
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Brocade Security Advisory ID: BSA-2015-003
Initial Publication Date: April 24, 2015
Revision: 7.0
Revision Date: March 23, 2017

Component: OpenSSL
CVSS: 5.0

CVE-2014-3572: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3572

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.2.1.R5.
Brocade Fabric OS	Not impacted.
Brocade Network OS	Not impacted
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release, Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted - Users of Services Controller VAs 2.0 or earlier should upgrade to a newer version of the Services Controller. Users of Services Controller s/w installs should consult their OS vendors to ensure their systems are secure.
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Impacted – Fixed in 4.9-35119 and later releases.
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Brocade Security Advisory ID: BSA-2015-003
Initial Publication Date: April 24, 2015
Revision: 7.0
Revision Date: March 23, 2017

Component: OpeSSL
CVSS: 5.0

CVE-2014-8275: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8275

OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.2.1R5.
Brocade Fabric OS	Not impacted
Brocade Network OS	Not impacted
Brocade NetIron OS	Impacted - Fixed in 5.9.0a and 6.0.0.
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Under investigation
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release, Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted - For users of s/w installs, should upgrade the version of OpenSSL on their system to an unaffected version.
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Not impacted
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Component: OpenSSL
CVSS: 4.3

CVE-2015-0204: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.5R2.
Brocade Fabric OS	Not impacted
Brocade Network OS	Not impacted
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Impacted - Fixed in SI12.4.00r, SI12.5.01e, and SI12502d.
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release, Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted - Upgrade to a newer version of the Services Controller. Users of Services Controller s/w installs should consult their OS vendors to ensure their systems are secure
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Impacted – Fixed in 4.9-35119 or newer.
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Brocade Security Advisory ID: BSA-2015-003
Initial Publication Date: April 24, 2015
Revision: 7.0
Revision Date: March 23, 2017

Component: OpenSSL
CVSS: 5.0

CVE-2015-0205 - https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0205

The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.2.1.R5.
Brocade Fabric OS	Impacted - Fixed in 8.0.1.
Brocade Network OS	Impacted - Fixed in 6.0.2.
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release, Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted - Users of Services Controller VAs 2.0 or earlier should upgrade to a newer version of the Services Controller. Users of Services Controller s/w installs should consult their OS vendors to ensure their systems are secure.
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Not impacted
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Component: OpenSSL
CVSS: 5.0

CVE-2015-0206 - https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0206

Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R7.
Brocade 5600 vRouter	Impacted - Fixed in 3.2.1R5.
Brocade Fabric OS	Not impacted
Brocade Network OS	Not impacted
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Impacted - Upgrade appliances to version 10.1 and later. Fixed in 9.9r1 for customers using the 9.9 LTS release, Brocade vTM software customers are not affected.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Impacted – Users of Services Controller VAs 2.0 or earlier should upgrade to a newer version of the Services Controller. Users of Services Controller s/w installs should consult their OS vendors to ensure their systems are secure.
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Impacted – Upgrade to 4.9-35119 or newer, which includes openssl-1.0.1k or newer.
Brocade Network Advisor	Not impacted
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

BROCADE

Disclaimer

Document Revision	Changes
1.0	Initial Publication
2.0	Updated for Fabric OS and vRouter 5400
3.0	Change table format, added CVE information
4.0	Updated to address BigIron and Virtual ADX
5.0	Updated to address NetIron OS
6.0	Updated to address Fabric OS, Network OS, Jetcore, ADX, Virtual ADX, Traffic Manager, Services Director, Firewall, BNA, and IronView
7.0	Updated to address Virtual ADX