Brocade Security Advisory ID: BSA-2016-005
Initial Publication Date: April 11, 2016
Revision: 3.0
Revision Date: March 27, 2017

BROCADE ®

Component: TCP Sequence Number
CVSS Score: 5.0

CVE-2004-0230: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230

TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Not impacted
Brocade 5600 vRouter	Impacted - Fixed in 4.2R1.
Brocade Fabric OS	Impacted - Linux is vulnerable. But the security impact is not important. Both Redhat and Debian are not fixing this.
Brocade Network OS	Impacted - Linux is vulnerable. But the security impact is not important. Both Redhat and Debian are not fixing this.
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Not impacted
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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: Staprun
CVSS Score: 4.4

CVE-2011-2502: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2502

runtime/staprun/staprun_funcs.c in the systemtap runtime tool (staprun) in SystemTap before 1.6 does not properly validate modules when a module path is specified by a user for user-space probing, which allows local users in the stapusr group to gain privileges via a crafted module in the search path in the -u argument.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Not impacted
Brocade 5600 vRouter	Not impacted
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Not impacted
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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: PHP
CVSS Score: 7.5

CVE-2012-0911: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0911

TikiWiki CMS/Groupware before 6.7 LTS and before 8.4 allows remote attackers to execute arbitrary PHP code via a crafted serialized object in the (1) cookieName to lib/banners/bannerlib.php; (2) printpages or (3) printstructures parameter to (a) tiki-print_multi_pages.php or (b) tiki-print_pages.php; or (4) sendpages, (5) sendstructures, or (6) sendarticles parameter to tiki-send_objects.php, which is not properly handled when processed by the unserialize function.

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Not impacted
Brocade 5600 vRouter	Not impacted
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Not impacted
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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: NTP
CVSS Score: 6.4

CVE-2015-7704: https://access.redhat.com/security/cve/CVE-2015-7704

Denial of Service by Spoofed NTP Kiss-o'-Death

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted - Fixed in 6.7R12.
Brocade 5600 vRouter	Impacted - Fixed in 4.1R1.
Brocade Fabric OS	Not impacted
Brocade Network OS	Not impacted
Brocade NetIron OS	Under investigation
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
Brocade 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 - Brocade vTM software customers are not affected. Brocade vTM appliance customers should upgrade to version 10.3 or later. Alternatively, for customers using the 9.9 LTS release, the fix is included in 9.9r1.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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

BROCADE

Component: NTP
CVSS Score: 2.6

CVE-2015-7975: https://access.redhat.com/security/cve/CVE-2015-7975

NTP nextvar() missing length check

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted – Fixed in 6.7R13.
Brocade 5600 vRouter	Impacted – Fixed in 5.0R1.
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Not impacted
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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

BROCADE

Component: NTP
CVSS Score: 4.0

CVE-2015-7976: https://access.redhat.com/security/cve/CVE-2015-7976

ntpq saveconfig command allows dangerous characters in filenames

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted – Fixed in 6.7R13.
Brocade 5600 vRouter	Impacted – Fixed in 5.0R1.
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Under investigation
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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

BROCADE

Component: NTP
CVSS Score: 4.3

CVE-2015-7977: https://access.redhat.com/security/cve/CVE-2015-7977

NTP Reslist NULL pointer dereference

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted – Fixed in 6.7R13.
Brocade 5600 vRouter	Impacted – Fixed in 5.0R1.
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Under investigation
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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

BROCADE

Component: NTP
CVSS Score: 5.8

CVE-2015-7979: https://access.redhat.com/security/cve/CVE-2015-7979

Off-path Denial of Service (DOS) attack on authenticated broadcast mode. More at:
http://support.ntp.org/bin/view/Main/SecurityNotice#January_2016_NTP_4_2_8p6_Securit

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted – Fixed in 6.7R13.
Brocade 5600 vRouter	Impacted – Fixed in 5.0R1.
Brocade Fabric OS	Not impacted
Brocade Network OS	Not impacted
Brocade NetIron OS	Under investigation
Brocade FastIron OS	Not impacted
Brocade BigIron RX	Not impacted
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Under investigation
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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

BROCADE

Component: NTP
CVSS Score: 6.4

CVE-2015-8139: https://access.redhat.com/security/cve/CVE-2015-8139

Origin Leak: ntpq and ntpdc, disclose origin

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted – Fixed in 6.7R13.
Brocade 5600 vRouter	Impacted – Fixed in 5.0R1.
Brocade Fabric OS	Not impacted
Brocade Network OS	Not impacted
Brocade NetIron OS	Not impacted
Brocade FastIron OS	Impacted – Fixed in FI08.0.50.
Brocade BigIron RX	Not impacted
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Brocade vTM software releases do not contain the vulnerability. Brocade vTM appliance customers are recommended to ensure their NTP configuration is such that the time is acquired from multiple sources.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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

BROCADE

Component: NTP
CVSS Score: 5.4

CVE-2015-8140: https://access.redhat.com/security/cve/CVE-2015-8140

ntpq vulnerable to replay attacks

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted – Fixed in 6.7R13.
Brocade 5600 vRouter	Impacted – Fixed in 5.0R1.
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Brocade vTM software releases do not contain the vulnerability. Brocade vTM appliance customers are recommended to ensure their NTP configuration is such that the time is acquired from multiple sources.
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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

BROCADE

Component: NTP
CVSS Score: 4.3

CVE-2015-8158: https://access.redhat.com/security/cve/CVE-2015-8158

Potential Infinite Loop in ntpq

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Impacted – Fixed in 6.7R13.
Brocade 5600 vRouter	Impacted – Fixed in 5.0R1.
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Under investigation
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
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 Score: N/A

CVE-2016-0701: https://mta.openssl.org/pipermail/openssl-announce/2016-January/000061.html

DH small subgroups

Product	Current Assessment
Brocade SDN Controller	Not impacted
Brocade 5400 vRouter	Not impacted
Brocade 5600 vRouter	Not impacted
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
Brocade ServerIron JetCore	Not impacted
Brocade ADX Series	Not impacted
Brocade Virtual ADX	Not impacted
Brocade Virtual Traffic Manager (formerly Brocade SteelApp Traffic Manager (STM))	Not impacted
Brocade Services Director (formerly SteelApp Services Controller (SSC))	Not impacted
Brocade Virtual Web Application Firewall (formerly Brocade SteelApp Application Firewall (SAF))	Not impacted
Brocade Network Advisor	Impacted - Upgrade to BNA 14.0.1.
Brocade IronView Network Manager	Not impacted
Brocade Data Center Fabric Manager	Not impacted

Brocade Security Advisory ID: BSA-2016-005
Initial Publication Date: April 11, 2016
Revision: 3.0
Revision Date: March 27, 2017

BROCADE⊠

Disclaimer

THIS DOCUMENT IS PROVIDED ON AN AS-IS BASIS SOLELY FOR INFORMATIONAL PURPOSES AND DOES NOT IMPLY ANY KIND OF GUARANTY OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. YOUR USE OF THE INFORMATION CONTAINED HEREIN IS AT YOUR OWN RISK. ALL INFORMATION PROVIDED HEREIN IS BASED ON BROCADE'S CURRENT KNOWLEDGE AND UNDERSTANDING OF THE VULNERABILITY AND IMPACT TO BROCADE HARDWARE AND SOFTWARE PRODUCTS. BROCADE RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Document Revision	Changes
1.0	Initial Publication
2.0	Updated to address v5400 Router, v5600 Router, FastIron, and Virtual Traffic Manager
3.0	Updated to address NetIron