



AT&T

AT&T Vyatta 5400 vRouter Software Patches

June 1, 2018



The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change. It is not for use or disclosure outside of AT&T companies except under written agreement.

© 2018 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners.



Contents

AT&T Vyatta 5400 vRouter Patches	4
6.7R14 (Rancho Cordova)	4
6.7R14S1	4
6.7R14S2	4
6.7R14S3	4
6.7R14S4	5
6.7R14S5	5
6.7R14S6	5
6.7R14S7	6
6.7R14S8	7



AT&T Vyatta 5400 vRouter Patches

This document lists the patches for the Vyatta 5400 vRouter.

6.7R14 (Rancho Cordova)

6.7R14S1

Released September 22, 2017.

Issue number	Priority	Summary
VSE-9841	Major	CVE-2017-0663, CVE-2017-7376: Debian DLA-1060-1: libxml2 security update
VSE-9840	Major	CVE-2017-1000100: Debian DLA-1062-1: curl security update
VSE-9839	Major	CVE-2017-11185: Debian DLA-1059-1: strongswan security update
VSE-9835	Major	CVE-2017-7522, CVE-2017-7521, CVE-2017-7520, CVE-2017-7508 OpenVPN security update
VSE-9831	Major	MTU setting reverts back to default after reboot on a vif interface

Issues resolved in 6.7R14S1

6.7R14S2

Released October 10, 2017.

Issue number	Priority	Summary
VSE-9845	Critical	CVE-2017-14491, CVE-2017-14492, CVE-2017-14494: Debian DLA-1124-1: dnsmasq security update
VSE-9837	Minor	"show system commit different" showing permission denied after upgrade from 6.7R11S9 to 6.7R13S3

Issues resolved in 6.7R14S2

6.7R14S3

Released November 14, 2017.



Issue number	Priority	Summary
VSE-9856	Major	CVE-2017-7805: Debian DLA-1138-1: nss security update
VSE-9852	Blocker	CVE-2017-13089, CVE-2017-13090: Debian DLA-1149-1: wget security update

Issues resolved in 6.7R14S3

6.7R14S4

Released Decemgber 19, 2017.

Issue number	Priority	Summary
VSE-9857	Minor	CVE-2017-10672: DLA-1171-1 libxml-libxml-perl – security update

Issues resolved in 6.7R14S4

6.7R14S5

Released February 2, 2018.

Issue number	Priority	Summary
VSE-9875	Critical	CVE-2018-5764: Debian DLA-1247-1: rsync security update
VSE-9866	Minor	IPsec out of sequence inbound errors
VSE-9864	Critical	CVE-2017-15412: Debian DLA-1211-1: libxml2 security update
VSE-9802	Major	CVE-2017-9022, CVE-2017-9023: Debian DLA-973-1: strongswan security update

Issues resolved in 6.7R14S5

6.7R14S6

Released March 6, 2018.

Issue number	Priority	Summary
VSE-9887	Major	CVE-2018-5334, CVE-2018-5335, CVE-2018-5336: Debian DSA-4101-1: wireshark – security update



Issue number	Priority	Summary
VSE-9884	Major	Tcpdump security update
VSE-9883	Major	Debian DLA-1291-1: tzdata new upstream version
VSE-9880	Minor	Disabling RPF source-validation does not remove setting from all interfaces
VSE-9878	Minor	CVE-2018-1000007: Debian DLA-1263-1: curl security update
VSE-9871	Critical	CVE-2017-5754: Debian DSA-4078-1: linux – security update (Meltdown)
VSE-9867	Major	CVE-2017-17405, CVE_2017-17790: Debian DLA-1221-1: ruby1.0.1 security update
VSE-9852	Blocker	CVE-2017-13089, CVE-2017-13090: Debian DLA-1149-1: wget security update
VSE-9851	Critical	CVE-2017-1000257: Debian DLA-1143-1: curl security update
VSE-9850	Minor	CVE-2017-10140: Debian DLA-1135-1: db security update
VSE-9817	Minor	CVE-2017-1000366 Plugin: 100875 Debian DLA-992-1: eglibc security update

Issues resolved in 6.7R14S6

6.7R14S7

Released May 14, 2018.

Issue number	Priority	Summary
VSE-9897	Major	CVE-2017-17742, CVE-2018-1000075, CVE-2018-1000076, CVE-2018-1000077, CVE-2017-1000078, CVE-2018-6914, CVE-2017-8777, CVE-2018-8778, CVE-2018-8779, CVE-2018-8780: Debian DLA-1358-1: ruby1.9.1 security update
VSE-9896	Minor	CVE-2018-7322, CVE-2018-7323, CVE-2018-7324, CVE-2018-7332, CVE-2018-7334, CVE-2018-7335, CVE-2018-7336, CVE-2018-7337, CVE-2017-7417, CVE-2018-7418, CVE-2018-7419, CVE-2018-7420: Debian DLA-1353-1: wireshark security update
VSE-9895	Major	CVE-2018-1000156: Debian DLA-1348-1: patch security update
VSE-9894	Major	CVE-2018-6913: Debian DLA-1345-1: perl security update



Issue number	Priority	Summary
VSE-9893	Major	CVE-2018-0739: Debian DLA-1330-1: openssl security update
VSE-9892	Major	CVE-2017-12627: Debian DLA-1328-1: xerces-c security update
VSE-9891	Major	Debian DLA-1323-1: tzdata security update
VSE-9890	Minor	CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122: Debian DLA-1309-1: curl security update
VSE-9886	Major	CVE-2017-17512: Debian DSA-4071-01: sensible-utils – security update
VSE-9885	Minor	CVE-2017-3735, CVE_2017-3736: DSA-4018-1 openssl – security update
VSE-9832	Major	CVE-2017-11185: Debian DLA-1059-1: strongswan security update
VSE-9525	Minor	Show version gives “SMBIOS” error message

Issues resolved in 6.7R14S7

6.7R14S8

Released June 1, 2018.

Issue number	Priority	Summary
VSE-9905	Major	CVE-2018-11358, CVE-2018-11362, CVE-2018-9258, CVE-2018-9260, CVE-2018-9261, CVE-2018-9263, CVE-2018-9268, CVE_2018-9269, CVE-2018-9270: Debian DLA-1388-1: wireshark security update
VSE-9902	Minor	CVE-2018-1000301: Debian DLA-1379-1: curl security update
VSE-9899	Minor	CVE-2018-0494: Debian DLA-1375-1: wget security update

Issues resolved in 6.7R14S8