VYATTA, INC. | Release Notes

Vyatta Release 6.3-2011.08.31

August 2011

Document Part No. A0-0095-10-30

Vyatta
1301 Shoreway Road
Suite 200
Belmont, CA 94002
vyatta.com

Contents

These release notes document changes made for Release 6.3-2011.08.31.

Security

The following security vulnerabilities have been addressed in this release:

CVE-2011-2748: ISC DHCP Server Halt.

> A vulnerability existed in DHCP server that caused it to halt if it processed certain packets. The vulnerability has been resolved by discarding or properly processing the packets. This issue is recorded as Bug ID 7467.

CVE-2011-0997: DHCP: dhclient does not strip or escape shell meta-characters.

> A vulnerability existed in DHCP client where it did not strip or escape certain shell meta-characters in responses from the DHCP server. This could result in execution of exploit code on the client. The vulnerability has been resolved. This issue is recorded as Bug ID 7467.

Bug ID 7378: Kernel crash when receiving malformed TCP packet

> A vulnerability existed where a deliberately malformed TCP packet could cause the kernel to halt. The vulnerability has been resolved in Bug ID 7378.

New in This Release

This release of the Vyatta system includes features for the Vyatta Subscription Edition.

The following new features are available for the Vyatta Subscription Edition:

- **Vyatta system virtual appliance for Red Hat KVM.** The Vyatta system now supports the Kernel-Based Virtual Machine (KVM) hypervisor on Red Hat Enterprise Linux version 6.1 (RHEL 6.1), packaged as a prebuilt virtual appliance. Like other virtualization platforms, the Red Hat KVM provides the ability to run multiple virtual systems on a single hardware platform. Instructions for installing and upgrading the Vyatta KVM virtual appliance are provided in a new guide, *Installing and Upgrading for Red Hat KVM.*

- **Vyatta system as an AMI.** The Vyatta system is now available as an Amazon Machine Image (AMI) for use with Amazon Web Services (AWS). You can launch the Vyatta AMI into a virtual private cloud (VPC) within the AWS cloud and access the Vyatta system remotely. Instructions for installing and upgrading the Vyatta AMI, as well as configuration examples, are provided in a new guide, *Amazon Machine Image Installation and Operations Guide.*

Behavior Changes

There are no behavior changes in this release.

Documentation Changes

To support the introduction of the Vyatta system KVM virtual appliance, a new guide has been developed: "*Installing and Upgrading for Red Hat KVM.*"

To support the introduction of the Vyatta system for Amazon Web Interface, a new guide has been developed: "*Amazon Machine Image Installation and Operations Guide.*"

Upgrade Notes

FULL-UPGRADE COMMAND DEPRECATED

The package upgrade method of upgrading and the "full-upgrade" command are **no longer supported**. Image-based upgrade is now the only supported upgrade method for physical systems. If you are upgrading in a virtualized environment, use the procedures specific to virtual system upgrade described in the *Vyatta Installation and Upgrade Reference Guide*.

DISK SPACE REQUIREMENTS

If you are upgrading from VSE6.1, please ensure that you have enough disk space to upgrade, as the system does not automatically detect lack of space and notify you. This issue is corrected in releases post-VSE6.1.

DOUBLE-QUOTE CHARACTERS IN CONFIGURATION

If you are upgrading a system that uses the double quote (") character in a value string within the configuration, you must remove the configuration lines containing the double quote character before upgrading. Some such lines can be replaced with functionally equivalent configuration after the upgrade. Failure to do so can render the system inaccessible once it is upgraded.

The double quote character is sometimes used in free-form text values such as the openvpn-option, DHCP global-parameters and shared-network-parameters, system login banner, and interface description values. Some instances can be worked around using alternate configuration. For example, the configuration:

```
interfaces openvpn vtunX openvpn-option “--push “route 10.254.0.0 255.255.0.0””
```

can be replaced after upgrade with either:

```
interfaces openvpn vtunX openvpn-option “--push route 10.254.0.0 255.255.0.0”
```

or:

```
interfaces openvpn vtunX server push-route 10.254.0.0/16
```

Instances that cannot be worked around must be removed from the configuration prior to upgrading.

MIGRATION OF CONFIGURATION DATA

Release 6.2 changed the location of certain configuration information. If you are upgrading from VSE6.2 or an earlier release, you must perform a migration procedure to preserve configuration information for some features. Affected features are as follows:

- Web proxy and URL filtering (Vyattaguard database and the community blacklists)
- Intrusion prevention (community rules and SNORTVRT subscriptions)
- Configuration parameters that reference file locations from the CLI (for example, WAN load-balancing hook, OpenVPN and L2TP/IPsec certificates, IPsec and RSA keys, and so on)

If you are not using these features, you can skip the procedures below.

These procedures will store your data in a manner consistent with the ongoing image-upgrade process. The procedures only need to be performed once; subsequent upgrades do not require them.

URL-filtering/Web Proxy

To preserve web proxy information, copy the required URL-filtering files from the old image to the new image.

Upgrade to the new image, following the procedures in the *Vyatta System Installing and Upgrading Reference Guide.* This is the “running system.”

1. If your web proxy uses the VyattaGuard database, restore configuration as follows:

   - If it exists, delete the directory **/config/url-filtering/sitefilter/** on the running system, as follows:

     ```
     delete file running://config/url-filtering/sitefilter/
     ```

   - Copy the file *image-name***://var/lib/sitefilter/** (where *image-name* is the name of the pre-upgrade image; for example, **VSE6.2-2011.04.06**), to **/config/url-filtering/sitefilter/** on the running system, as in the following example:

     ```
     copy file VSE6.2-2011.04.06://var/lib/sitefilter/ to  running://config/url-filtering/sitefilter/
     ```

2. If your web proxy uses a community blacklist, restore configuration as follows:

   - On the running system, delete the directory **/config/url-filtering/squidguard/**, as follows:

     ```
     delete file running://config/url-filtering/squidguard/
     ```

   - Copy the file *image-name*:**//var/lib/squidguard/** (where *image-name* is the name of the pre-upgrade image) to **/config/url-filtering/squidguard/** on the running system, as in the following example:

     ```
     copy file VSE6.2-2011.04.06://var/lib/squidguard/ to  running://config/url-filtering/squidguard/
     ```

3. Restart your system to reload configuration.

Intrusion Prevention System

To preserve IPS information, copy the required IPS files from the old image to the new image.

1. Upgrade to the new image, following the procedures in the *Vyatta System Installing and Upgrading Reference Guide.* This is the "running system." Have the files from the old image available to you.

2. Copy the file *image-name*:**//opt/vyatta/etc/ips/snortrules-snapshot-***num***.tar.gz** (where *image-name* is the name of the pre-upgrade image and *num* is the number of your Snort rules database. The following example copies the Snort version 2.8.5.3 rule set from image VSE6.2-2011.04.06 to the running system:

   ```
   copy file VSE6.2-2011.04.06://opt/vyatta/etc/ips/snortrules-snapshot-2583.tar.gz
   to  running://config/ips/snortrules-snapshot-latest.tar.gz
   ```

3. Restart your system to reload configuration.

Scripts and Certificates

To preserve script and certificate information, three steps are required after upgrading to the new image:

1. Copy certificates and scripts to the new directory.

2. Update any configuration node referencing the script to use the new path.

3. Restart your system to reload configuration.

As an example, the following procedure migrates X.509 certificates. In this example, the certificates on the old image reside in **/opt/vyatta/etc/certs/x509** and are copied to the **x509** subdirectory in **/config/auth**.

1. Upgrade to the new image, following the procedures in the *Vyatta System Installing and Upgrading Reference Guide.* This is the "running system." Have the files from the old image available to you.

2. Copy the certificates, as follows:

   ```
   copy file VSE6.2-2011.04.06://opt/vyatta/etc/certs/x509/ to
   running://config/auth/x509/
   ```

3. Restart your system to reload configuration.

The following example migrates a script called **wlb-hook**. In the example, this script is referenced in the **load-balancing wan hook** configuration node using the absolute path **/home/vyatta/wlb-hook**.

1. Upgrade to the new image, following the procedures in the *Vyatta System Installing and Upgrading Reference Guide.* This is the "running system." Have the files from the old image available to you.
2. Copy the file *image-name***://home/vyatta/wlb-hook** (where *image-name* is the name of the pre-upgrade image; for example, **VSE6.2-2011.04.06**), to **/config/scripts/wlb-hook** on the running system.

```
copy file VSE6.2-2011.04.06://home/vyatta/wlb-hook to
running://config/scripts/wlb-hook
```

3. In WAN load balancing configuration, modify the **load-balancing wan hook** node to have the value of the new path: **/config/scripts/wlb-hook**.

```
configure
set load-balancing wan hook / config/scripts/wlb-hook
commit
exit
```

4. Restart your system to reload configuration.

Resolved Issues

The following issues have been resolved in this release.

Bug ID	Severity	Description
Bridging		
7164	3 - major	STP does not stabilize when a bridging loop is present
CLI		
7362	3 - major	variable references made using relative path in syntax:expression return empty values incorrectly when user is not at top-level in configuration hierarchy
Configuration Syncronization		
7444	6 - enhancement	Config-sync should verify version of remote system prior to syncing and fail if version string does not match that of primary
DHCP		
7377	4 - minor	DHCP client lease is not removed following the deletion of DHCP client from an interface
Firewall		
7477	3 - major	firewall group negation doesn't work in vc6.3 and vse6.3
Interfaces		
7382	3 - major	Deletion of interface address dhcp (dhclient) followed by a commit of a static address creates an out of sync condition between the configuration and the running system

7408	1 - blocker	interfaces ethernet needlessly forces MAC address causing interfaces to flap on commit
7453	7 - unassigned	disabled interface fills log with dhclient error messages
Kernel		
7378	2 - critical	kernel crash when receiving malformed TCP packet
Security Issues		
7467	7 - unassigned	Upgrade ISC DHCP per security advisories
SNMP		
7366	4 - minor	Errors "Warning: Unknown token: smuxpeer", "Warning: Unknown token: smuxsocket" from snmpd on boot with SNMP configured
7403	3 - major	SMUX communication between SNMPd and Quagga routing protocol MIBs is broken
URL Filtering		
7371	3 - major	url_init: database expired message reported for valid VyattaGuard entitlement
7485	4 - minor	no default value for url-filtering auto-update node
VPN		
7440	3 - major	Unable to modify L2TP configuration on cluster standby if ipsec is configured as a cluster service
7465	5 - trivial	Show commands don't properly handle 3des encryption method

Known Issues

Bug ID	Description
AMI	
7449	For an instance outside of a Virtual Private Cloud (VPC), if the instance is stopped and started again, it is no longer possible to access the instance using SSH. Recommended action: If SSH is the desired connection method, make sure your instances reside within the VPC.
7450	"Failed to read ..." errors can display on the console when an AMI instance boots. Recommended action: None. This issue is display-only.
BGP	
5822	The "neighbor <peer-group-name> ebgp-multihop 255" configuration entry appears in the routing engine after committing “delete peer-group <peer-group-name> remote-as <>". This issue only occurs when the peer-group remote-as is the same as the local one, i.e., the peer-group is iBGP. Recommended action: Remove the peer group entirely; alternatively, issue the following command vtysh –c 'conf t' -c 'router bgp *local-asn*' -c 'no neighbor *peer-group-name* ebgp-multihop'
6030	Currently, BGP redistribution is not supported for both IPv4 and IPv6 at the same time. Recommended action: None.
6042	The BGP "confederation peers asn" option cannot be used after the peer's ASN configuration has already been committed. Recommended action: None.

6817	A "delete protocols bgp <>" operation fails to commit when “redistribute” and "address-family ipv6-unicast" are configured. Recommended action: Delete either of the two latter options first, then delete BGP configuration in its entirety.
7493	The BGP process crashed after a BGP neighbor with a peer group is deleted and the configuration change is commited. Recommended action: None.
CLI	
2654	Non-privileged commands are shown to users in help. A number of commands that cannot be executed by non-privileged users (“operator” users) are displayed as valid commands and are completed with tab completion. Recommended action: Please note that the “configure” and “install-system” commands are not available to users with “operator” role. Recommended action: None.
2777	Stray quote confuses CLI. Accidentally typing a single quote puts the CLI into a mode where it expects additional input, as in the following example: root@charon# set interfaces ethernet eth' [edit] root@charon# commit > > > This occurs in both operational and configuration mode. Recommended action: Avoid typing stray single quotes when entering commands. Note: This is currently designed behavior. For more information about using the Vyatta CLI, please see the “Using the CLI” chapter of the *Vyatta Basic System Reference Guide*.
6902	Using the double quote (") character in a value string within the configuration can cause the configuration to fail when it is loading. This can cause an inability to login after an upgrade, for example. Recommended action: Prior to upgrading, check your configuration for the double quote (“) character. It is typically used in conjunction with the openvpn-option and dhcp-server option commands. Some instances can be worked around using alternate commands. For example, the command: interfaces openvpn vtunX openvpn-option “--push “route 10.254.0.0 255.255.0.0”” can be replaced with interfaces openvpn vtunX server push-route 10.254.0.0/16 Instances that cannot be worked around must be removed from the configuration prior to upgrading.
7267	I-node exhaustion artificially limits the number of sets (or size of the loaded config) in a single commit. Recommended action: Run 'commit' more frequently so that no more than a few hundred 'sets' are applied in each commit.
7331	In previous releases, comments from a configuration migration could be removed by saving the configuration after a successful boot. This is no longer possible, because the “save” command no longer ignores comments. Recommended action: None.
Clustering	
3105	If two clustered routers reboot when the master router's monitored interface is down, the master still becomes active.

	This issue occurs only when both routers are booting and the master's monitored interface is disabled in configuration. After the routers come up, master negotiates to active even though its interface is disabled. If the interface is enabled, traffic flows normally. If the interface is disabled again, the routers fail over as expected. This issue does not occur if fewer than 15 services are entered in the cluster. This issue does not occur if the two routers are rebooted with a gap of 30 seconds or greater. Recommended action: Reboot the primary router, or delete the cluster configuration on the primary router and reload the configuration.
DHCP	
2657	Lease expiration is not displayed in local time; it is displayed in GMT timezone only irrespective of the system’s configured timezone. Recommended action: None.
DHCPv6	
6844	Currently DHCPv6 doesn't properly distribute options when using SLAAC for addresses. A way to distribute these options is by making them global for the DHCP server instead of under a subnet block. Adding these options will give the DHCPv6 server more flexibility, and will make configuration easier if the options for an organization are the same for all subnets. Recommended action: None.
Firewall	
5065	A commit error is generated if a firewall “name” configuration is deleted at the same time as deleting the assignment of the firewall “name” to an interface. Recommended action: Delete the assignment and commit the change, then delete the “name” configuration and commit the change.
6965	The "show firewall" command returns incorrect information for 'packets' and 'bytes' after some million packets are traversed. Recommended action: None.
7139	Enhancement request: The experimental "firewall modify" feature should be tested, documented, and supported. Recommended action: None.
IDS	
7182	Content inspection can fail when the IPv6 protocol is blacklisted. Recommended action: Avoid specifying IPv6 as a blacklisted protocol.
Installer	
6135	An error occurs when the install-system command is executed at the point where the default root partition size is chosen and the install fails. Recommended action: If this problem occurs, manually select a partition size slightly smaller than the size reported by the drive. Install should subsequently be successful.
Interfaces	
4983	Wanpipe ADSL Link status reads "Disconnected , 0x1" while link is connected on some circuits. Recommended action: None.
6714	A vif interface cannot be deleted if it belongs to a bridge. Recommended action: To avoid this problem, delete the vif’s bridge configuration before deleting the vif itself.
Kernel	
5295	Connection tracking helper modules cannot re-assemble application layer PDUs residing in two or more TCP segments. This is typically only a problem when an application layer PDU is larger than 1500 bytes. The result of this issue is that the application can fail. Recommended action: None.

NAT	
5678	“show nat translations monitor” cannot currently be used to continuously monitor both source and destination NAT translations together. Recommended action: Monitor source and destination NAT translation separately using “show nat translations source monitor” and “show nat translations destination monitor”.
OpenVPN	
7387	If an OpenVPN tunnel is added to a bridge group and the commit fails, the tunnel remains part of the bridge group. Recommended action: None
7388	It is currently possible to configure an OpenVPN tunnel on top of a socket that is in use by an existing OpenVPN tunnel, An error occurs when the configuration is committed. Ideally, a message should indicate this error when the configuration is being created rather than waiting until commit time. Recommended action: None
OSPF	
3004	Deleting an OSPF area may fail if the network entry is not a connected network and virtual links are in use. The configuration commit fails with an "Area does not exist" error message. Recommended action: Remove virtual links included in an OSPF area configuration prior to deleting the OSPF area.
3348	OSPF process dies if the router ID value is modified while OSPF routers are converging. This issue may also occur after convergence if the OSPF router ID is changed twice within a short interval. Recommended action: If the OSPF router ID must be changed, it must be changed after OSPF routers have finished converging, when OSPF adjacencies are stable and OSPF routes in the RIB are synced with OSPF LSAs.
6762	A “delete protocols ospf” operation fails if the “passive-interface-exclude” option has been configured. Recommended action: Delete the “passive-interface-exclude” configuration setting before deleting OSPF configuration.
Policy	
6166	Configuration commit fails when a route-map is deleted using the “comm-list” option. Recommended action: To avoid this problem, do not attempt to delete using the “comm-list” option if it is already set. Alternatively, use the “set community” command with values that exclude the community to be deleted.
PPP	
6609	When a high-load test is performed with a four-link multilink PPP bundle on Sangoma A104 cards, a receive-side panic occasionally occurs, with the panic signature beginning as follows: 487.026549] BUG: unable to handle kernel NULL pointer dereference at (null) Recommended action: None.
Serial	
4983	On some circuits, the Wanpipe ADSL Link status shows as "Disconnected , 0x1" even though the link is connected. Recommended action: None. This issue is display-only.
5724	Serial interfaces cannot be recreated once they are deleted. Recommended action: If this problem occurs, reboot the system and it will be possible to recreate the interface.
SNMP	
5442	64-bit SNMP traffic counters do not work for all ethernet interfaces Recommended action: Use SNMP OIDs for 32-bit counters instead of 64-bit for unsupported

	interfaces.
6789	No response to SNMP request if the reverse path forwarding check fails. In certain network topologies, the system does not respond to SNMP requests. This problem occurs when the packet containing the SNMP request arrives on one interface, but the system's active route to the request's source IP goes through a different interface. In these situations, the reverse path forwarding filter fails and the request is dropped. Recommended action: Depending on your network topology, you can use either of the following methods to avoid this issue: • Send SNMP requests to an IP address on the interface facing the next hop on the route back to your SNMP client. • Add a route from the router to the SNMP client's address or network so that the route to the client uses the same interface which the request arrives through.
7183	Packet capture results indicate that the source address of SNMP trap is not changed if the address is set or modified. Even if the trap source is configured, the system uses its own IP address as the source IP of the trap. Recommended action: None.
Static Routes	
5905	If the distance for a static IPv6 route is updated or deleted, the change is not recorded in the routing engine. Recommended action: Delete the route, then set it again with the new distance.
System	
5792	When the “show system image”, “show system image version”, and “show system image storage” commands are executed on a system deployed from a LiveCD, the system displays the following message: "Can not open Grub config file." No other information is displayed, and in particular, it is not clear that the issue is storage. The message should inform the user that it is not valid to run these commands on a LiveCD. Recommended action: None.
6825	A memory leak can occur in the connection tracking mechanism. This can lead to page allocation failure. Recommended action: None.
6952	The system reports the following message if it boots immediately prior to receiving a login prompt: ata2: failed to resume link (SControl 0) Recommended action: None. This issue is display-only.
7072	Enhancement request: The Vyatta software supports two upgrade mechanisms: the package-based "full-upgrade" method and image-based upgrade. There should be one consistent, reliable upgrade path between Vyatta versions. Recommended action: None.
Virtual Environment	
7398	Deactivating a network interface from within the guest settings Network tab causes the XenServer guest account to crash with a kernel panic. Recommended action: To avoid this issue, use the Vyatta CLI to disable the network interface.
VPN	
6839	A configuration change to the “ipsec vpn pre-shared-secret” configuration option does not take effect immediately as it should. Recommended action: Restart the VPN process after changing the pre-shared secret, using the “restart vpn” command.

7084	A "restart vpn" command will fail with large numbers of configured tunnels. The maximum number of tunnels that can be configured depends on the hardware resources available on the system. Recommended action: None.
7087	The PPTP and L2TP VPN services, it is possible to create local users without specifying a password and have the users be authenticated. Recommended action: Ensure that every local-user under "vpn remote-access" is assigned a password.
7092	The IPsec daemon fails if more than 301 interface addresses are configured. Recommended action: None.
7456	IPSec VPN peers relying on name resolution do not work properly, because the name resolution for the peer is incorrect. Recommended action: To work around this issue, configure the local peer using the following format: @*name*.*domain*.xxx Where *name* is the name to be resolved and *domain.xxx* is the domain. On the remote peer, configure the authentication ID identically (i.e., @*name*.*domain*.xxx).
VRRP	
1819	Allow VRRP set to same address as interface address with auto 255 priority. Recommended action: None
6843	When the “conntrack sync” option is enabled, changing the size of the conntrack table causes the VRRP process to reload. Recommended action: If conntrack-sync is enabled, perform conntrack-table size changes only within a disruptive maintenance window whenever possible.
7093	With keepalived version 1.2.2, the VRRP “clear vrrp master” command does not work correctly, such that the expected 0 priority packet is not sent out; instead, IGMP leave/join messages are observed and three seconds later, the backup router takes over. Recommended action: None.
Web GUI	
7239	The “delete system image” operation is not working on the web GUI. Recommended action: Use "delete system image ..." from the command line interface only.
7258	The Interactive command “generate->vpn->x509->key-pair” fails to execute. Recommended action: Use "generate vpn x509 ..." from the command line interface only.
7228	If HTTPS listen-address configuration is committed, the GUI fails. Recommended action: Modify the "service https listen-address" from the command line interface only.
7354	When Safari is used as the web browser, duplicate requests are sent to the server. Recommended action: None.
Web Proxy	
4952	If the web proxy feature is configured together with clustering, both configurations may be lost. Recommended action: None.