Security Bulletin

DNS Proxy Vulnerability on Internet Connected Routers/Gateways

In recent weeks there have been an increasing number of reports of “Denial of Service” attacks against publically connected Internet devices. These attacks which can affect most any device (including potentially Digi cellular devices) target DNS proxy servers and other services that have not been properly configured or secured. The potential result is overage charges resulting from high cellular data usage. This document describes how to prevent these attacks from affecting cellular data usage on Digi Connect and ConnectPort***** devices and what Digi is doing to further protect against such attacks.

It is important to note these attacks do *not* make the router vulnerable to break-in or allow access to the attached network. These attacks are simply someone attempting to disrupt service and/or generate excessive data usage.

(* - See the end of this document for information on Digi TransPort devices.)

How a DNS Proxy Server Attack Happens

“Bad actors” on the Internet attempt to send excessive DNS lookup requests, often for non-existent or malformed hosts. A router listens for DNS requests (UDP port 53) on all available interfaces, including the WAN interface. The offending DNS requests are sent, in this case, to the Digi unit via its wireless WAN interface. The DNS proxy feature forwards the DNS request to the servers in the DNS server list. Replies are returned, which are then forwarded to the client that originated the request. That transmits 4 UDP packets altogether, likely all over the wireless WAN connection. The attack is a constant barrage of DNS requests to the Digi’s WAN IP address, which results in excessive data usage.

Securing Digi Connect and ConnectPort Devices

To protect your Digi Connect and ConnectPort, Digi has the following recommendations to limit and monitor connectivity to the device. Refer to built-in WebUI help and/or the Digi User Guide for details.

- **Turn off all unused network services** on the device. Via Web UI go to *Configuration > Network > Network Services Settings* or via the CLI “*show service*” command. Use the “*set service*” command to change/disable services.
- **Enable IP Filtering** (Access Control List):
    a. Create a list of devices and/or networks which need to connect to the unit. Via the Web UI go to *Configuration > Network > IP Filtering Settings* or via CLI “*set access*”. Specific IP addresses like 55.66.77.88 or network address like 200.100.50.0 / 255.255.255.0 can be entered. The network entry gives access to any device on that network.
    b. Note for iDigi, if the device is configured for “client-initiated” connection, the IP address of the iDigi gateway is automatically added when the connection is established and deleted when removed.
- **Disable the DNS Proxy Service**:
    a. Via the Web UI go to *Configuration > Network > Advanced Network Settings*.

b. Under DNS Proxy Settings, *uncheck "Enable DNS Proxy Service*"
c. Enter static DNS server address(es) if required. Use known Internet-based DNS servers or addresses supplied by your network administrator.

- **Enable Usage Alarms**:
  a. In the WebUI go to *Configuration > Alarms*
  b. Select an alarm to use
  c. Select "*Send alarms based on cellular data exchanged …"* and configure *how much data* in what *period of time* deemed appropriate. Select *total* for cell data type.
  d. Select how to send the alarm via any or all of *SNMP, email, SMS text* (assuming your data plan supports SMS)
- **Use a private wireless WAN plan**. Some carriers provide plans that do not traverse or touch the Internet. Check with your carrier on availability.

What We are Doing to Help Further: Network Port Scan Cloaking

First, the DNS Proxy Service is disabled by default with Digi Connect / ConnectPort firmware version 2.12.0.6 going forward.

In addition, firmware version 2.12.0.6 will introduce a new feature: **Network Port Scan Cloaking**. This feature basically hides cloaked services from the WAN so they do not respond. It is configured via Web UI *Configuration > Network > Advanced Network Settings > Network Port Scan Cloaking*. These settings also may be managed via CLI (*set/show/revert/display scancloak*) and RCI. The <scan_cloak> settings group in the RCI includes RCI descriptors that can be used via iDigi to produce a configuration management display for these settings as well.

Network Port Scan Cloaking is enabled by default on Wireless WAN interfaces for most protocols. Cloaking is not enabled for other network interfaces (Ethernet, Wi-Fi).

Cloaking on WAN interfaces is intentionally not enabled by default for *ping* replies since pings are a useful diagnostic tool. Cloaking for ping can be enabled if desired, or use custom defaults to do so.

Cloaking can be applied to the device by groups and protocols. A group is either a global (device-wide) selection or a network interface. The global selection is available for all products with the cloaking feature enabled in them. The specific network interfaces that appear as groups, depends upon how a particular product is manufactured (which interfaces are available in that product). Possible groups include:

- global (all network interfaces)
- eth0 (Ethernet), eth1 (Ethernet)
- wln0 (WiFi)
- mobile0 (cellular)
- wmx0 (WiMAX)

In addition to the ability to configure cloaking by group, it also may be configured by individual protocol. The protocols include:

- Ping
- TCP
- UDP
- DNS Proxy

If cloaking is enabled, the network stack will take these actions:

- Ping – do not reply to ping requests
- TCP – do not send TCP RST (reset) responses to received TCP packets that do not correspond to a local port or service.
- UDP – do not send ICMP destination/port unreachable packets in response to received UDP packets that do not have a local port or service.
- DNS Proxy – do not process DNS requests received on a network interface for which cloaking is enabled for the DNS Proxy feature.

Received packets that are filtered by cloaking are discarded by the network stack. Statistics on the cloaking discards may be viewed by use of the CLI “display scancloak” command.

The initial state of cloaking at boot time, and subsequent changes to it, are reported in the event log. The logged messages are to the “system” facility. The logged message text is clear in that it pertains to the Network Port Scan Cloaking feature.

Individual discarded packet occurrences can be traced (to the “treck” trace mask at the debug level), but not logged to the event log. Under an attack, recording cloak discards to the event log would become overwhelming in volume.

Refer to the Digi’s WebUI built-in *Help* link, located in the upper right corner of the screen, for details.

How iDigi Manager Pro Can Help

Digi’s device management service, iDigi Manager Pro, can securely monitor and manage 100s or 1000s of devices from your browser. Instead of requiring a log into each device individually to make the above changes; iDigi Manager Pro allows you to make a configuration change once and then send the updated configuration to all units. Firmware updates are just as easy. To try iDigi Manager Pro for a free 30 day trial, call +1 877-iDigi-EZ (1-877-434-4439).

See www.idigi.com for more details.

Addendum: Securing a Digi TransPort

Digi TransPort routers use an operating system different than Digi Connect devices (both proprietary and secure) and therefore have different security configurations. The TransPort has a ***stateful firewall*** used to block and translate addresses and services.

The easiest and most direct way to secure a Digi TransPort router is to enable and configure the firewall to block any unsolicited inbound traffic on the appropriate cellular, wireless or wired WAN interface. For example, the cellular interface on Digi TransPort WR series uses PPP 1; on TransPort DR it is PPP 3 (the DSL modem is on PPP 1).

Below is a sample TransPort firewall file. Inbound traffic is blocked unless matches a rule. Outbound DNS queries are allowed from the LAN, but any DNS queries from the WAN will be ignored. So, the hacker will try once or twice and then give up.

```
#Allow outbound FTP traffic
pass out break end proto ftp from any to any port=ftpcnt flags S!A inspect-state
#Allow any other outbound traffic and the replies back in
pass out break end inspect-state
#Allow incoming IPSEC
pass break end proto 50
pass in break end proto udp from any to any port=ike
pass in break end proto udp from any to any port=4500
#Allow any traffic within an IPSEC tunnel in both directions
pass break end oneroute any
#Allow incoming SSH and SFTP on alternate SSH port 8022
pass in break end proto tcp from any to any port=8022 flags S!A inspect-state
#Allow incoming HTTPS
pass in break end proto tcp from any to any port=443 flags S!A inspect-state
#Block and log everything else including incoming telnet, http and FTP
block log break end
```