

## TCP Vulnerability: BGP Session termination by spoofed TCP RST

April 23, 2004

Version 1.2

A new TCP vulnerability was identified on Tuesday April 20, 2004 regarding the ability to DoS attack any router or host by successfully sending a spoofed packet with the correct 4-tuple TCP IP header information, with a valid packet sequence number that the end device will accept, for an existing established session. According to the TCP standard, when a valid packet with the RST bit set is received, the router or host receiving the packet will kill the established session. This vulnerability affects all Foundry equipment and applications that support TCP connections, including Foundry switches.

In past, this attack was very near impossible as the possibilities of guessing the rotating sequence number is  $1/2^{32}$ . The new vulnerability shows us that the next sequence range can be calculated and successfully guessed in as low as 4 attempts and can succeed within seconds. This information is reportedly being made public on Thursday, April 22, 2004. Serious attacks may be attempted on customer networks thereafter.

The attack is most harmful against long lived TCP sessions that cause broader actions to occur if the session terminates prematurely. The primary target of this attack is BGP peering sessions. BGP sessions are long lived and have large TCP window sizes - allowing the attack to be successful. The persistent nature of a BGP peering session gives sufficient time for enough spoof packets to be sent with randomly selected sequence numbers. The large window size allows for taking advantage of a feature of TCP stacks that allows the next sequence number to be any value between the last sequence number received + 1 and the last sequence number received + the window size. The DoS robot generates randomly selected sequence numbers from various ranges and uses them in the spoofed session with a higher probability that one of these packets will look valid to the end device. The increased probability of successfully taking advantage of the TCP vulnerability has caused the urgent announcement.

When a telnet or ssh session is terminated, the user will usually re-initiate the session with no lasting effect. When a BGP peering session is terminated, it causes other actions to occur within the BGP protocol. Resetting the connection can result in medium term unavailability due to the need to rebuild routing tables and induce a "route flapping" condition. Route flapping may result in route dampening, which may affect the ability to route to segments of the network.

For more information on this vulnerability, please refer to:

<http://www.uniras.gov.uk/vuls/2004/236929/index.htm>

### Foundry's BGP Solution

Foundry's BGP technology can be fully protected by using the MD5 hash protection feature. Foundry highly recommends that our BGP customers implement MD5 protection as soon as possible to protect their connections against this type of attack. With BGP MD5 protection turned on, Foundry routers will drop the spoofed packet before it can do any damage as the MD5 signature is checked first and the spoofed packet should not be able to reproduce the MD5 signature.

An example configuration for enabling MD5 for a BGP neighbor and a peer group are as follows:

```
BigIron(config-bgp-router)# local-as 2
BigIron(config-bgp-router)# neighbor xyz peer-group
BigIron(config-bgp-router)# neighbor xyz password abc
BigIron(config-bgp-router)# neighbor 10.10.200.102 peer-group xyz
BigIron(config-bgp-router)# neighbor 10.10.200.102 password test
```

Here is how the configuration will appear when using the show command. The passwords are shown encrypted for security reasons.

```
BigIron(config-bgp-router)# show ip bgp config
Current BGP configuration:
router bgp
  local-as 2
  neighbor xyz peer-group
  neighbor xyz password 1 $!2d
  neighbor 10.10.200.102 peer-group xyz
  neighbor 10.10.200.102 remote-as 1
  neighbor 10.10.200.102 password 1 $on-o
```

The MD-5 authentication must be enabled on each neighbor using the same password string. This feature interoperates with other vendors MD-5 implementations.

The BGP with MD-5 authentication was introduced in software release 7.1.14 and all subsequent releases contain this feature.

## Foundry ServerIron Solution

Foundry's ServerIron products when enabled for Global Server Load Balancing (GSLB) use Foundry's internal GSLB protocol to communicate information between GSLB site and controller devices. TCP connections are used for this communication, and these TCP sessions can be protected through the GSLB MD5 authentication feature. This feature is supported in ServerIron versions 8.2R. As BGP is not supported on the ServerIron platform, it is not vulnerable to the BGP type of attacks this vulnerability is targeting on network infrastructure gear.

To turn on MD5 protection on the ServerIron platform, perform the following (refer to the ServerIron TrafficWorks 8.2.00R Release Notes for complete details):

User needs to enable GSLB authentication and configure the authentication password on the GSLB Controller and the Site ServerIrons. The authentication password should be same on all the ServerIrons for which authentication is desired.

To enable authentication for the GSLB protocol and to configure the password for authentication, configure the following on the GSLB ServerIron and the Site ServerIrons:

```
ServerIron#conf t
ServerIron(config)#gslb auth-enable 0 secureauthenticationpassword
ServerIron(config)#end
```

**Syntax: `gslb auth-enable <code> <password>`**  
**<code>:**

The possible values for code are 0, 1 or 255

### Configuring the TCP port for GSLB authentication

By default, GSLB ServerIron will use TCP port 183 to exchange authenticated GSLB information with Site ServerIrons. You can change the GSLB protocol port used for authenticated messages, if needed.

To change the TCP port for authentication, configure the following on the ServerIron:

```
ServerIron#con t
```

```
ServerIron(config)#gslb auth-encrypt-communication 2000
Reload required. Please write memory and then reload or power cycle.
ServerIron(config)#
```

**Syntax: gslb auth-encrypt-communication <tcp-port-number>**

**<tcp-port-number>**: Refers to TCP port number for exchange of authenticated protocol messages. Default value is 183.

Note that a reload is required for this command to take effect.

**Specifying Site ServerIrons that support authentication and/or encryption**

To specify the Site ServerIrons for which only authentication should be enabled, configure the following at the Site level on the GSLB ServerIron:

```
GSLB-ServerIron#con t
GSLB-ServerIron(config)#gslb site new
GSLB-ServerIron(config-gslb-site-new)#auth-only-list 1.1.1.116
GSLB-ServerIron(config-gslb-site-new)#end
```

**Syntax: gslb auth-only-list <IP addresses>**

**<IP address>**: *This refers to the list of ServerIron IP addresses at a Site for which the GSLB protocol messages will only be authenticated but not encrypted.*

**Foundry Patch**

Foundry is currently working on a patch that will prevent this vulnerability from guessing a valid sequence number in the TCP Sequence Window. This will further safeguard against this vulnerability in addition to the other safeguards mentioned above. For more information in this RFC, refer to the following link:

<http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt>

Foundry will post this patch on its support web site when completed:

<http://www.foundrynet.com/services/support/index.html>

**Additional Recommendations**

As a precaution, customers should check their switches and routers to make sure the management IP addresses are not accessible from the Public Internet. Using ACL's or other Foundry Security Features to limit access to remote management protocols and to turn off unnecessary management protocols should seriously be considered. Implementing anti-spoofing ACL's should also be considered for all public facing router ports and other high risk router ports as a precautionary measure.

For more information on hardening your Foundry infrastructure, please refer to the following White Paper, "IronShield Best Practices: Hardening Foundry Routers & Switches".

<http://www.foundrynet.com/solutions/security/index.html>

## **References**

US-CERT

Technical Cyber Security Alert TA04-111A Vulnerabilities in TCP  
<http://www.us-cert.gov/cas/techalerts/TA04-111A.html>

National Infrastructure Security Co-ordination Center

NISCC Vulnerability Advisory 236929 Vulnerability Issues in TCP  
<http://www.uniras.gov.uk/vuls/2004/236929/index.htm>

IETF Internet Draft

<http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt>