Table of Contents

Cisco Security Notice: Response to Cisco PIX TCP Connection Prevention

Document ID: 68268

http://www.cisco.com/warp/public/707/cisco−response−20051122−pix.shtml

Revision 1.0

For Public Release 2005 November 28 1900 GMT (UTC)

Please provide your feedback on this document.

Cisco Response

This is Cisco PSIRT's response to the statements made by Arhont Ltd.− Information Security in its message: [Full−disclosure] Cisco PIX TCP Connection Prevention, posted on November 22, 2005.

The original email is available at
http://lists.grok.org.uk/pipermail/full−disclosure/2005−November/038971.html

This issue is being tracked by two Cisco Bug IDs:

- **CSCsc14915** −− PIX 6.3 Spoofed TCP SYN packets can block legitimate TCP connections
  This Bug ID tracks the issue for PIX software version 6.3 and older. This DDTS is under investigation and while not resolved there are workarounds available to mitigate the issue.
- **CSCsc16014** −− PIX 7.0 Spoofed TCP SYN packets can block legitimate TCP connections
  This Bug ID tracks the issue for PIX/ASA software version 7.0. This DDTS is under investigation and while not resolved additional mitigations and workarounds exist to limit or eliminate the issue.

We would like to thank Arhont Ltd.− Information Security for reporting this issue to us.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

Additional Information

PIX 6.3

CSCsc14915 −− PIX 6.3 Spoofed TCP SYN packets can block legitimate TCP connections

This issue affects PIX software version 6.3 and older. The Release Note Enclosure for this Bug ID states:

Symptom:

TCP connections through the firewall may be silently blocked.

Conditions:

By sending a TCP SYN packet with an incorrect checksum through a PIX firewall, the PIX will block new TCP connections using the same source and destination TCP ports and IP addresses. Connections will remain blocked for approximately two minutes after which connections will be allowed. This behavior may be seen on all firewall interfaces but can be expected to have the most impact on TCP connections originating from higher security level interfaces to lower security level interfaces.

Since the spoofed packets have an incorrect checksum, they are silently discarded by the destination and the firewall will not see a RST packet from either the destination or the legitimate source and will hold the embryonic connection open until the embryonic connection timeout which is 2 minutes by default.

The root cause is due to the spoofed packet creating an embryonic connection which sets up the TCP sliding window. A valid packet from a real host using the same connection as the spoofed packet sends a SYN over the same connection. The sequence number of the valid packet is out−of−window and rejected by the firewall's TCP sequence number check. Any subsequent retransmissions of the valid packet are also out−of−window and are rejected by TCP sequence number check.

Other spoofed TCP SYN packets that create embryonic connections can also cause this behavior, blocking legitimate TCP connections until the embryonic connection times out.

Workaround:

Issuing the commands **clear xlate** or **clear local−host <ip address on the higher security level interface>** will allow the firewall to pass connections again.

TCP connections discarded because of this issue can be verified by enabling **debug fixup tcp**. 'Out of Window' drops will then generate messages that begin with **"tcpseq: discard old packet"**. Debug messages may impact firewall performance and should be tested before being enabled in a production environment.

For discarded TCP connections originating from lower security level interfaces to higher security level interfaces, **TCP Intercept** can be configured on **STATIC** commands by setting the **emb_limit** to 1. This results in the PIX proxying all connection attempts after the first connection. The PIX will create and send the TCP SYN,ACK from the destination to the original source. Since the original TCP SYN packet was spoofed, the source IP address will not be tracking the TCP connection and it will send a TCP RST to the PIX. The PIX will then close the connection originating from the TCP SYN packet with the incorrect checksum. TCP Intercept may impact firewall performance and should be tested before being enabled in a production environment.

Further Problem Description:

PIX software version 6.3 does not verify the TCP checksum of packets transiting through the firewall.

Because the PIX does not verify the TCP checksum, the malformed TCP packet is allowed through the firewall in a half−opened, embryonic state.

The destination host discards the received malformed segments. Because the firewall does not see a return segment from the destination host it holds the half−open TCP connection open until the embryonic timeout which is set to two minutes for PIX 6.3 and earlier software.

Because the firewall is holding a connection open, any additional packets with the same protocol, IP addresses, and ports will be treated as part of the existing half−open connection. In this case, a legitimate SYN packet following the malformed SYN will be discarded because it is outside of the window of acceptable sequence numbers established by the malformed packet.

For information on configuring the emb_limit as part of the **STATIC** command in PIX software version 6.3 refer to:

STATIC

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/cmdref/s.htm#wp1026694

PIX/ASA 7.0

CSCsc16014 −− PIX 7.0 Spoofed TCP SYN packets can block legitimate TCP connections

This issue affects PIX/ASA software version 7.0. Additional mitigations and workarounds to limit or eliminate the issue. The Release Note Enclosure for this Bug ID states:

Symptom:

TCP connections through the firewall may be silently blocked.

Conditions:

By sending a TCP SYN packet with an invalid checksum through a PIX firewall, the PIX will block new TCP connections using the same source and destination TCP ports and IP addresses. Connections will remain blocked until the embryonic connection timeout which is 30 seconds by default. This behavior may be seen on all firewall interfaces but can be expected to have the most impact on TCP connections originating from higher security level interfaces to lower security level interfaces.

Since the spoofed packets have an invalid checksum, they are silently discarded by the destination and the firewall will not see a RST packet from either the destination or the legitimate source and will hold the embryonic connection open until the embryonic connection timeout which is 30 seconds by default.

The root cause is due to the spoofed packet creating an embryonic connection which sets up the TCP sliding window. A valid packet from a real host using the same connection as the spoofed packet sends a SYN over the same connection. The sequence number of the valid packet is out−of−window and rejected by the firewall's TCP sequence number check. Any subsequent retransmissions of the valid packet are also out−of−window and are rejected by TCP sequence number check.

Other spoofed TCP SYN packets that create embryonic connections can also cause this behavior, blocking legitimate TCP connections until the embryonic connection times out.

This behavior can be verified by issuing the command: **show asp drop**.

The counter for "TCP RST/SYN in window" or "TCP SEQ in SYN/SYNACK invalid" should increment for every packet dropped in this manner.

Workarounds:

Several workarounds exist for this issue.

1. Issuing the commands **clear xlate** or **clear local−host <ip address on the higher security level interface>** will allow the firewall to pass connections again.
2. The default TCP embryonic connection timeout is 30 seconds. This default can also be modified which further mitigates the issue. This workaround should be effective regardless of the cause of the issue.
   This configuration example sets the TCP embryonic connection timeout to 10 seconds for the default "global_policy" policy−map:

   ```
   access−list tcp_inspection extended permit tcp any any
   access−list tcp_inspection extended deny ip any any

   class−map my_inspection_tcp
    match access−list tcp_inspection

   policy−map global_policy
    class my_inspection_tcp
     set connection timeout embryonic 0:00:10

   service−policy global_policy global
   ```
3. **TCP Intercept** can be configured to allow the PIX to proxy all TCP connection attempts originated from behind any firewall interface after the first connection. PIX will create and send the TCP SYN,ACK from the destination to the original source. Since the original TCP SYN packet was spoofed, the source IP address will not be tracking the TCP connection and it will send a TCP RST to the PIX. The PIX will then close the connection originating from the TCP SYN packet with the invalid checksum. This workaround should be effective regardless of the cause of the issue.
   This example proxies all TCP connection attempts originated from any firewall interface after the first connection for the default "global_policy" policy−map:

   ```
   access−list tcp_inspection extended permit tcp any any
   access−list tcp_inspection extended deny ip any any

   class−map my_inspection_tcp
    match access−list tcp_inspection

   policy−map global_policy
    class my_inspection_tcp
     set connection embryonic−conn−max 1

   service−policy global_policy global
   ```
4. When invalid checksums are the cause of this issue, PIX/ASA software version 7.0 can be configured to verify TCP checksums which will eliminate the impact. Verifying TCP checksums may impact firewall performance and should be tested before being enabled in a production environment.
   This example verifies TCP packet checksums for the default "global_policy" policy−map:

   ```
   tcp−map verify−chksum
     checksum−verification

   access−list tcp_inspection extended permit tcp any any
   access−list tcp_inspection extended deny ip any any

   class−map my_inspection_tcp
    match access−list tcp_inspection

   policy−map global_policy
    class my_inspection_tcp
     set connection advanced−options verify−chksum

   service−policy global_policy global
   ```

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at http://www.cisco.com/go/psirt.

Updated: Nov 28, 2005 Document ID: 68268