PureSecurity
Security Advisory

Advisory: Check Point VPN-1 SecuRemote DoS/Spoofing Attack for Site-Site VPN
Release Date: 2008/03/17
Last Modified: 2008/03/17
Author: Robert Mitchell <rdm@puresecurity.com.au>
Application: Check Point VPN-1
Versions: Tested on R65, confirmed by vendor on R65 HFA 02
(other versions likely to be affected, although not tested.)
Attack type: Denial of Service, VPN Tunnel takeover causing information leakage.
Risk: Medium
Vendor Status: Vendor advised, hotfix available.
References: Check Point SecureKnowledge article ID sk34579
(to be published)

Overview:

A SecuRemote user can break connectivity for a Site-Site VPN from the same VPN Gateway. If SecuRemote back-connections are enabled and the rulebase allows, the Site-Site tunnel traffic can be re-routed to the SecuRemote client.

Details:

Scenario is as follows:

* VPN-1 Gateway (NGX R65) has a site-site tunnel to a 3rd party. Remote party's tunnel endpoint IP a.b.c.d is in the remote encryption domain.

* VPN-1 Gateway also is a termination point for SecuRemote users. SecuRemote site is set up for IP Pool NAT.

* SecuRemote user has the IP address of a.b.c.d installed as the local IP address on their machine, behind a NAT device e.g. an ADSL modem/router.

When the user connects, VPN-1 establishes a User tunnel to the IP address a.b.c.d. This tunnel breaks connectivity for the site-site VPN.

If Back Connections are enabled, the Site-Site tunnel is replaced by a Site-Client tunnel, and, depending on the rulebase construction, information that was supposed to flow down the Site-Site tunnel is sent to the Client instead.

Vendor response:

Vendor advised through support and Security Alert channels on 20th February. Issue acknowledged and reproduced by vendor. Vendor hotfix available 12th March on request.

Proof of Concept:

Main NGX R65 Gateway IP - 1.2.3.4
Internal network - 10.1.0.0/16

Remote VPN Site
Remote Internal VPN domain - 192.168.1.0/24 - target IP 192.168.1.10

SecuRemote User

Public IP Address 5.6.7.8
User is NATted by ADSL modem (or equivalent). The IP address on User's computer is 192.168.1.10.

1. Set up Local Site VPN Topology. Use IP Pools for SecuRemote.

2. Set up Externally Managed VPN Site or Interoperable VPN Device and Site.

3. Set up two VPN Communities - one for Remote Access, another for Site-Site. Disable NAT on the communities. It does not appear to matter if the Tunnel management is per-host or per-subnet.

4. Set up rules for remote access and VPN transfers. Place a rule for general outbound access below these rules.

5. Install SecuRemote on a Client PC. Place this behind an ADSL modem or similar, so that a private address can exist as the IP on the SR machine.

6. Install policy and test that Site-Site and Remote access VPNs work with independent addresses.

7. Change SecuRemote PC IP to 192.168.1.10.

8. Connect to VPN with SecuRemote. Use a profile that doesn't allow/use Office Mode.

9. From the Internal network, try and connect. SecuRemote will connect, and connections to the Site-Site tunnel 192.168.1.10 address will fail.

10. Enable back connections for SecuRemote. Connect from Internal network to 192.168.1.10. Connection will go to SR host on the outbound access rule.

Discussion:

What appears to happen is a conflict between the Phase 2 SAs created for Site-Site and Client-Site tunnels. In essence, the DoS and the tunnel takeover
happens because the phase 2 negotiation of the Client-Site tunnel overwrites or takes priority over the previous Site-Site phase 2 negotiation, and subsequently the traffic originally destined for the Site-Site tunnel on the

target address no longer matches the Site-Site VPN domain.

The exposure is mitigated because a valid SecuRemote user account and reasonably good knowledge of the network topology is required.

However, the impact may be severe. The capacity to use SecuRemote connections with NAT to negotiate tunnels for arbitrary source addresses, even those that conflict with other sessions, and thus intercept VPN traffic or even masquerade as another host inside the hijacked VPN is daunting.

The safest workaround is to use Check Point's Office Mode features, to control the inner source IP of the client-site tunnel. This is Check Point's recommended solution, and does not at this stage appear to be vulnerable to the same attack.

Solutions and Work-arounds:

- Vendor provided hotfix for VPN-1 NGX R65 12th March.
- Force all SecuRemote/SecureClient users to use Office Mode. If you're not using Office Mode, don't turn on back connections.

Disclosure Timeline:

20.	February 2008	- Contacted Checkpoint by email
22.	February 2008	- Vendor response.
12.	March 2008	- Vendor hotfix supplied
13.	March 2008	- Vendor hotfix tested and validated.
16.	March 2008	- Minor revisions based on vendor feedback.
17.	March 2008	- Vulnerability Published and distributed to Secunia and CERT.

Acknowledgements

Thanks to Mitchell Woodward for his assistance in testing.
PureSecurity acknowledges Michael Kapelevich and the Check Point Security Alert team for their prompt response and open dialogue on this issue.