

[NEWS] Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0007.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/05/04

To: list@securiteam.com

Date: 5 Feb 2004 19:06:03 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow

SUMMARY

"Checkpoint VPN-1 server and Checkpoint VPN clients (SecuRemote/SecureClient) collaborate to provide VPN access to corporate networks for remote client computers. VPN-1 is the VPN component commonly deployed on Checkpoint Firewall-1 installations. The IKE component of these products allows for the unidirectional or bidirectional authentication of two remote nodes as well as the negotiation of cryptographic capabilities and keys."

A buffer overflow condition has been found when attempting to handle large certificate payloads. A remote attacker may exploit this flaw to remotely compromise any VPN-1 server and/or client system running SecureClient/SecureClient. Successful compromise of the VPN-1 server can lead directly to complete compromise of the entire Checkpoint Firewall-1 server.

DETAILS

Vulnerable Systems:

* VPN-1 Server 4.1 up to and including SP6 with OpenSSL HotFix

Securiteam: [NEWS] Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow

* SecuRemote/SecureClient 4.1 up to and including build 4200

Immune Systems:

* Firewall-1 NG FP1 or greater

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0040>>
CAN-2004-0040

Internet Key Exchange (IKE) is used to negotiate and exchange keys for encrypted transport or tunneling of network traffic over a Virtual Private Network (VPN). The network protocol used to facilitate this exchange is the Internet Security Association and Key Management Protocol (ISAKMP).

The vulnerability exhibits itself when handling ISAKMP packets with large Certificate Request payloads. This can be triggered by a remote unauthenticated attacker during the initial phases of an IKE negotiation.

It is not necessary to impersonate a known VPN server to exploit client systems, and VPN servers are equally vulnerable. As this attack does not require any interaction with the target system, it can be performed via UDP with a spoofed source address concealing the identity of an attacker.

There is insufficient bounds checking and a classic stack overflow is possible. From there the way is paved for remote code execution and hence full compromise of the server.

Workaround

There is no effective workaround for this vulnerability. Upgrading to the NG versions of VPN-1 Server and SecuRemote/Client will remove this vulnerability. Checkpoint no longer supports the versions of VPN-1 and SecuRemote/SecureClient affected by this vulnerability. Checkpoint recommends that all affected users upgrade to Firewall-1 NG FP1 or greater.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:weld@vulnwatch.org>> Chris Wysopal.

The original article can be found at:

<<http://xforce.iss.net/xforce/alerts/id/163>>
<http://xforce.iss.net/xforce/alerts/id/163>.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.