

[NEWS] Cisco VPN Concentrator Groupname Enumeration Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0084.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/20/05

To: list@securiteam.com

Date: 20 Jun 2005 15:21:53 +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>

Cisco VPN Concentrator Groupname Enumeration Vulnerability

SUMMARY

NTA Monitor has discovered a groupname enumeration vulnerability in the Cisco VPN 3000 series concentrator products while performing a VPN security test for a customer.

The vulnerability affects remote access VPNs with groupname authentication. Site-to-site VPN operation is not affected, nor is remote access with certificate authentication. In practice, we find that most concentrators are configured for remote access with groupname authentication, so this bug will affect the majority of users.

The vulnerability allows an attacker to use a dictionary attack to determine valid group names on the concentrator. Once a valid group name is determined, the attacker can then use this to obtain a hash from the concentrator, which can then be cracked offline to determine the group password.

Once an attacker has a valid groupname and group password, they can potentially mount a Man-in-the-Middle (MitM) attack against the XAUTH user authentication mechanism. This allows the attacker to snoop on VPN

Securiteam: [NEWS] Cisco VPN Concentrator Groupname Enumeration Vulnerability

traffic, alter VPN traffic, or gain access to the network protected by the VPN. This MitM attack works even if strong authentication such as SecurID is used for user authentication.

DETAILS

Affected Versions:

The issue is believed to affect all models of Cisco VPN 3000 Concentrator: 3005, 3015, 3020, 3030, 3060 and 3080. We believe that all software versions prior to 4.1.7.F are vulnerable.

Technical Details:

The vulnerability allows an attacker to enumerate valid groupnames on a Cisco VPN concentrator through either a dictionary attack, or a brute-force attack. The issue exists because the concentrator responds to valid groupnames differently to the way in which it responds to invalid groupnames.

The exploit involves sending an IKE Aggressive Mode packet with the groupname to be tested in the Identity (ID) payload. The ID Type is 11, which corresponds to ID_KEY_ID. If the specified groupname is valid, the concentrator will respond; if it is not valid, then the concentrator will not respond. The ike-scan tool can be used to demonstrate this vulnerability.

The vulnerability is present in both normal IKE over UDP, and also Cisco proprietary TCP-encapsulated IKE. The ike-scan tool can use either transport type: for Cisco IKE in TCP, you need to specify the option `--tcp=2`. When using TCP encapsulation, an invalid groupname causes the concentrator to send a TCP RST packet, which causes ike-scan to return the error message "recvfrom: Connection reset by peer".

The groupname guessing rate depends on the bandwidth between the attacker's system and the concentrator. Because most of the group names tried will be incorrect, and therefore the concentrator won't respond, it's only the bandwidth from the attacker to the concentrator that matters; the bandwidth from the concentrator back to the attacker is not important.

An IKE aggressive mode packet with a single transform, using Diffie-Hellman group 2, and having an eight character groupname has an IKE packet size of 256 bytes. Adding the eight byte UDP header and 20 byte IP header gives a total size of 284 bytes or 2,272 bits. Assuming a link speed of 2Mbits/sec, this gives a guessing rate of $2,000,000 / 2,272 = 880$ guesses per second.

A guessing rate of 880 per second is 3,168,000 per hour or 76,032,000 per day. This rate is sufficient to perform an extensive dictionary attack, or a limited brute-force attack. The concentrator does not limit the groupname guessing rate, nor does it blacklist hosts that perform groupname enumeration: in tests, it was possible to get a successful

Securiteam: [NEWS] Cisco VPN Concentrator Groupname Enumeration Vulnerability

response to a valid groupname immediately after thousands of incorrect attempts.

Once a valid groupname is obtained, it is possible to use this groupname to obtain a hash from the concentrator, and mount an offline password-guessing attack against this hash to obtain the group password. Because the password-guessing process is offline, it is fast (hundreds of thousands of guesses per second), and will not cause the concentrator to log any authentication failures.

A valid groupname and password allows the attacker to complete IKE Phase-1 and establish an ISAKMP SA to the concentrator. They can then mount a Man-in-the-Middle (MitM) attack against the second-stage user-authentication process, which is typically XAUTH.

The offline password guessing process and MitM attack against XAUTH are detailed in the VPN flaws whitepaper at <http://www.nta-monitor.com/news/vpn-flaws/VPN-Flaws-Whitepaper.pdf>

Example:

The example below shows the two different concentrator responses: the first is for the valid groupname "finance", and the second is for the invalid groupname "administration". We see that the concentrator responds to valid groupname, but not to the invalid one. Because of this difference in behaviour, it is possible to determine whether a given groupname is valid or not.

The ike-scan options used in this example are:

- A Specify IKE Aggressive Mode. The default for ike-scan is Main Mode.
- idtype=11 Specify ID Type 11 for the ID payload. This corresponds to ID_KEY_ID.
- M Multiline: Display each payload on a separate line, which makes the output easier to read.
- auth=65001 Specify authentication method 65001, which corresponds to XAUTH.
- id=finance Specify the string to be used for the ID payload.
- 10.0.0.1 The IP address of the target VPN concentrator.

3.1. Response to valid groupname "finance":

```
$ ike-scan -A --idtype=11 -M --auth=65001 --id=finance 10.0.0.1
```

Starting ike-scan 1.7.2 with 1 hosts

(<http://www.nta-monitor.com/ike-scan/>)

10.0.0.1 Aggressive Mode Handshake returned

SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=XAUTH LifeType=Seconds LifeDuration=28800)

KeyExchange(128 bytes) Nonce(20 bytes) ID(Type=ID_IPV4_ADDR, Value=10.0.0.1) Hash(16 bytes)

VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)

VID=09002689dfd6b712 (XAUTH)

VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection)

Securiteam: [NEWS] Cisco VPN Concentrator Groupname Enumeration Vulnerability

VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

VID=65963c60eacf802220adccf628738746

VID=1f07f70eaa6514d3b0fa96542a500400 (Cisco VPN Concentrator)

Ending ike-scan 1.7.2: 1 hosts scanned in 0.423 seconds (2.36 hosts/sec).

1 returned handshake; 0 returned notify

3.2. Response to invalid groupname "administration":

```
$ ike-scan -A --idtype=11 -M --auth=65001 --id=administration 10.0.0.1
```

Starting ike-scan 1.7.2 with 1 hosts

(<http://www.nta-monitor.com/ike-scan/>)

Ending ike-scan 1.7.2: 1 hosts scanned in 0.594 seconds (1.68 hosts/sec).

0 returned handshake;

0 returned notify

Solution:

Upgrade to software version 4.1.7.F or later. Cisco customers with a valid login may obtain the new software from the Cisco website. Cisco has stated in the release notes that this software version is not vulnerable to the issue, but NTA Monitor have not verified this claim.

Alternatively, use certificate authentication rather than group authentication. This vulnerability does not apply to certificate authentication.

Timeline:

The vulnerability was first discovered on 8th July 2004, and was reported to Cisco's security team (PSIRT) on 20th September 2004. Cisco were able to reproduce the issue using the ike-scan tool, and bug ID CSCeg00323 was opened on 11th October 2004. Software version 4.1.7.F, which claims to have fixed the issue, was released on 19th May 2005.

References:

Cisco Bug ID CSCeg00323 "vpn3k - inconsistent behavior on scanning".NTA Monitor advisory

<<http://www.nta-monitor.com/news/vpn-flaws/cisco/VPN-Concentrator/index.htm>>

<http://www.nta-monitor.com/news/vpn-flaws/cisco/VPN-Concentrator/index.htm>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Roy.Hills@nta-monitor.com>>
Roy Hills.

The original article can be found at:

<<http://www.nta-monitor.com/news/vpn-flaws/VPN-Flaws-Whitepaper.pdf>>

<http://www.nta-monitor.com/news/vpn-flaws/VPN-Flaws-Whitepaper.pdf>

=====

Securiteam: [NEWS] Cisco VPN Concentrator Groupname Enumeration Vulnerability

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.