

Re: [Full-disclosure] Ciscos VPN-Client-Passwords can be decrypted

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-10/0225.html>

From: Clayton Kossmeyer (*ckossmey_at_cisco.com*)

Date: 10/18/05

Date: Tue, 18 Oct 2005 16:06:05 -0400

To: full-disclosure@lists.grok.org.uk

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hello –

The Cisco PSIRT is aware of reports that claim the Cisco VPN Client password encryption uses a breakable algorithm to encrypt user passwords.

We are aware of reports at the following sites:

<http://www.heise.de/newsticker/meldung/64954>

http://evilscientists.de/blog/?page_id=339

http://evilscientists.de/blog/?page_id=343

This issue is related to a Security Notice that the Cisco PSIRT released in October of 2004. Cisco's public announcement can be found here:

<http://www.cisco.com/warp/public/707/cisco-sn-20040415-grppass.shtml>

The Cisco VPN 3000 Series has a configuration option that does not allow the storage of the user password in the VPN client. For customers that are concerned about the recovery of the user password, the following option can be disabled to prevent local storage of the user password.

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a00803ee1f01

Cisco Client Parameters

Allow Password Storage on Client – Check this box to allow IPSec clients to store their login passwords on their local client

Re: [Full-disclosure] Ciscos VPN-Client-Passwords can be decrypted

SecurityFocus Bugtraq: Re: [Full-disclosure] Ciscos VPN-Client-Passwords can be decrypted

systems. If you do not allow password storage (the default), IPSec users must enter their password each time they seek access to the VPN. For maximum security, we recommend that you not allow password storage.

Note that the default configuration of the VPN 3000 Series does not allow client password storage. Additionally, this attack only affects passwords that are static and reused for login to the VPN network. Customers using one-time passwords (OTP) and certificates to connect are unaffected.

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

Regards,

Clay
Cisco PSIRT

On Sun, Oct 16, 2005 at 09:28:41PM +0200, Thierry Zoller wrote:

>
> *Dear List,*
>
> *[1] heise published a news article today.*
> *[2] EvilScientists reverse engineered the algorithm Cisco uses to _obscufate_ the*
> *passwords.*
> *[3] PoC*
>
> *Summary :*
> *Cisco uses 3des to encrypt the passwords, however it does so using*
> *a deterministic encryption scheme (no user input) and thus must be*
> *reproducible.*
>
> *The algorithm [2] found was as follows :*
>
> ** GetDate – convert to string*
> ** Generate an SHA Hash from that string h1 (20 Bytes)*
> ** h1 is modified into Hash h2*
> ** h1 is modified into Hash h3*
> ** h2 and the first 4 Bytes from h3 give the 3DES Key*
> ** The clear text password no encrypted in 3DES CBC Mode. The IV is the first 8 Bytes of h1.*
> ** If the size of the clear text password is not a multiple of the*
> *Block size, the differece to the next block is calculcated and padded*
> *with a Digit. -> length of password is known*
> ** A last hash is calculated from the encrypted Password h4*
> ** The value of the Key “enc_UserPassword” is: h1|h4|verschlüsselttes Passwort*
>
> *Credits:*

SecurityFocus Bugtraq: Re: [Full-disclosure] Cisco VPN-Client-Passwords can be decrypted

> [1] <http://www.heise.de/newsticker/meldung/64954>
> [2] http://evilscientists.de/blog/?page_id=339
> [3] <http://www.evilscientists.de/blog/?dl=CiscoPasswordRevealer.rar>
> I take no credit I am only translating and forwarding.
>
> --
> Thierry Zoller
> <http://thierry.sniff-em.com>
>
>
> _____
> Full-Disclosure – We believe in it.
> Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
> Hosted and sponsored by Secunia – <http://secunia.com/>
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.0 (SunOS)

iD8DBQFDVU8DEHa/Ybuq8nARAgVzAJ4mPsT5ThKc4DKJGAa76OuLSPs7CgCdFS+W
BjtwpXaQnRZvaR/UiH+/1wg=
=ivMN
-----END PGP SIGNATURE-----