

# [NEWS] Weak Cisco PIX Enable Password Encryption Algorithm

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0098.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 06/21/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Fri, 21 Jun 2002 21:15:50 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

Weak Cisco PIX Enable Password Encryption Algorithm

---

## SUMMARY

The encryption algorithm used by Cisco PIX Firewall software to encrypt passwords for "enable" and "passwd" commands is too easy (and fast) to calculate. An off-line password brute forcer has been found to be very effective in finding the plain text equivalent of the encrypted password.

## DETAILS

Vulnerable systems:

- \* Cisco PIX Firewalls (all models and all versions)

Cisco PIX passwords are limited to a length of 16 Bytes, so in theory there are  $255^{16}$  possible passwords, but in real life there are about  $80^{16}$  useful password combinations, take a look at your keyboard to verify, even if strong passwords are used.

Cisco's password encryption is based on base64 encoded MD5 hashes. Routers IOS uses 1000 MD5 Update rounds to make password brute forcing attacks harder, but the PIX firewall uses only one MD5 update and then the digest is base64 encoded.

## Securiteam: [NEWS] Weak Cisco PIX Enable Password Encryption Algorithm

For base64 encoding Cisco uses the `_crypt_to64()` Function of the FreeBSD `libcrypt` library.

Here's the code to compute PIX password hashes:

```
MD5Context ctx1;
unsigned char final[MD5_SIZE+1];
unsigned char cleartext [16+1];
unsigned char cisco_encoded [16+1];

memset(cisco_encoded,0,sizeof(cisco_encoded));
memset(cleartext,0,sizeof(cleartext));
strcpy((char*) cleartext,"test");

MD5Init2(&ctx1);
MD5Update2(&ctx1,(unsigned char*) cleartext,16);
MD5Final2(final,&ctx1);

char* p = (char*) cisco_encoded;
_crypt_to64(p,*(unsigned long*) (final+0),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+4),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+8),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+12),4); p += 4;
```

Due to weaknesses in the MD5 hash algorithm (den Boer and Bosselaers found a so called pseudo-collision) there may be more effective attacks methods in the future.

Impact:

PIX Firewalls are security devices principally used for perimeter security. Once gained access to the Firewall by mean of a valid enable password an intruder could modify its configuration as wanted. In this situation all networks and resources protected by the Firewall could be affected.

Another important impact is due to the ability of recent version of PIX Firewalls code (new feature in version 6.2) to sniff traffic. The "capture" command could be used by an intruder to perform a sniffing of remote traffic based on pre-configured ACLs.

Available Password Crackers:

Cain & Abel ( <<http://www.oxid.it>> [www.oxid.it](http://www.oxid.it))

Cain & Abel version 2.5 beta13 and above includes both crackers for Cisco PIX and Routers password hashes. The keyrate of those crackers shows the speed and feasibility of an off-line password guessing attacks.

Too many secrets ( <<http://www.ernw.de>> [www.ernw.de](http://www.ernw.de))

Version 0.9 includes password attacks (brute forcing, dictionary and hybrid attacks) for Cisco routers and the Cisco PIX firewall

Conclusions:

The feasibility of an off-line password guessing is something that every

Securiteam: [NEWS] Weak Cisco PIX Enable Password Encryption Algorithm

network administrator should consider before leaving PIX configuration files on TFTP servers, sending them unencrypted via email or using telnet for configuring the PIX.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[mao@oxid.it](mailto:mao@oxid.it)> mao and <mailto:[mthumann@ernw.de](mailto:mthumann@ernw.de)> Michael Thumann.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] Insecure Temporary Files in Acrobat Reader"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)