

Cisco Security Notice: Cisco PIX Password Encryption Algorithm

Document ID: 25483

For Public Release 2003 November 10

Please provide your feedback on this document.

Summary
Addressing the Report
Related Information

Summary

This is in response to an email sent by Michael Thumann and mao. The email is available at <http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html> and the subject is 'Weak Cisco PIX Password Encryption Algorithm'.

Addressing the Report

When considering the published report, consider the following:

- The password length and quality is very important.
Using passwords with ten characters or more make brute force attacks much harder up to the point when they become computationally unfeasible using the present algorithms and general purpose computers. Using passwords that are not easy to guess, with a mixture of lower and upper case letters and numbers, make off line dictionary attacks much harder.
- This attack is effective only if an attacker can capture the configuration file.
In order to prevent interception of the configuration files for the PIX, particularly during transfer between devices, customers should review their policies and practices concerning storage and transfer of PIX configuration files. Critical points of review should include firewall management systems and backup procedures (including media and disposal).
- By default, PIX does not accept interactive connections on any port except the console port.
Even if an attacker possesses the password, an interactive administrative session must be established to the trusted/protected (or externally via IPSec or SSH) interface of the PIX, in order to take advantage of this. Cisco configuration guides recommend explicit and careful configuration of permitted administrative hosts, and default configuration requires the administration hosts to be explicitly configured.
- Users are encouraged to use the local database that uses "salted" passwords. The example of a configuration is present here:

```
username <user> password <secret password>  
aaa authentication enable console LOCAL
```

Alternatively, users can consider using TACACS+ or RADIUS for authentication.

The practice of having a single, shared enable password should be discouraged in favor of creating a separate usernames with the appropriate privilege level. Additionally, a practice of sharing the same configuration file among multiple PIXes should be reconsidered. For the exact syntax of PIX command consult Cisco PIX Firewall Command Reference, Version 6.2.

Related Information

- [PIX Support Page](#)
 - [Documentation for PIX Firewall](#)
 - [PIX Command References](#)
 - [Requests for Comments \(RFCs\)](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 10, 2003

Document ID: 25483
