

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Advisories](#)

Cisco Security Advisory: PIX Private Link Key Processing and Cryptography Issues

Advisory ID: [cisco-sa-19980603-pix-key](#)

<http://www.cisco.com/warp/public/707/cisco-sa-19980603-pix-key.shtml>

Revision 1.1

Last Updated 1998 June 16 1500 UTC (GMT)

For Public Release 1998 June 3 1500 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Versions and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of This Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

PIX Private Link is an optional feature that can be installed in Cisco PIX firewalls. PIX Private Link creates IP virtual private networks over untrusted networks, such as the Internet, using tunnels encrypted with Data Encryption Standard (DES). PIX Private Link in versions up to 4.1 uses DES in ECB ("electronic codebook") mode.

An error in parsing of configuration file commands reduces the effective key length for the PIX Private Link DES encryption to 48 bits from the nominal 56 bits.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19980603-pix-key.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ **Affected Products**

This section provides details on affected products.

☐ **Vulnerable Products**

All users of the PIX Private Link encryption product with PIX software versions earlier than the date of this notice are affected. This includes all PIX Private Link software through version 4.1.6.

☐ **Products Confirmed Not Vulnerable**

No other Cisco products are currently known to be affected by these vulnerabilities.

[Top of the section](#) [Close Section](#)

☐ **Details**

This vulnerability has been assigned Cisco bug ID CSCdk11848. The use of ECB mode is Cisco bug ID CSCdj23353.

Affected Software Versions

This vulnerability affects all released versions of PIX Private Link software with version numbers up to and including 4.1.6, and all beta/interim software released earlier than the date of this notice.

Planned Software Fixes

The first regular release containing a fix for this problem will be version 4.2.1, which is tentatively scheduled for release in late June 1998. This schedule is subject to change. Fixes for the 4.1 software release have not yet been scheduled.

The 4.2.1 release also substitutes ECB mode with DES CBC mode.

Customers who need to upgrade immediately may contact Cisco's Technical Assistance Center (TAC) to obtain interim software. Interim software has not been subjected to full testing; it has a greater chance of containing serious bugs than would regular released software.

Interim releases are available only by special request from the Cisco TAC, not via the regular download channels. Cisco advises customers to install interim releases only if absolutely necessary. Customers who choose to install interim releases should plan to upgrade to the regular released

software when it becomes available.

When the fix is installed, it will be necessary to upgrade both ends of each Private Link tunnel at the same time. This is because the modified key parsing algorithm will lead old and new versions to derive different encryption keys from the same configuration file.

Software upgrades to correct this key-length problem will be offered free of charge to all PIX Private Link customers, regardless of their service contract status. Customers under contract may obtain upgrades through their usual procedures. Customers not under contract should call the Cisco TAC. Contact information for the TAC is in the "" section at the end of this message, and is available on Cisco's Worldwide Web site at <http://www.cisco.com/>.

The use of ECB mode was a deliberate design decision for the PIX Private Link product, and will not be changed. However, future IPSEC/IKE products for the PIX platforms will use other encryption modes.

[Top of the section](#) [Close Section](#)

▣ Impact

If attackers know the details of the key-parsing error in the PIX Private Link software, they will know 8 bits of the key ahead of time. This reduces the effective key length from the attacker's point of view from 56 to 48 bits. This reduction of the effective key length reduces the work involved in a brute-force attack on the encryption by a factor of 256. That is, knowledgeable attackers can, on the average, find the right key 256 times faster than they would be able to find it with a true 56-bit key.

In addition to this key-length issue, some customers have expressed concern over the use of DES ECB mode for PIX Private Link encryption. Although the use of ECB mode is intentional, ECB is not generally considered to be the best mode in which to employ DES, because it tends to simplify certain forms of cryptanalysis and may permit certain replay attacks. Technical details of the relative merits of various encryption modes are beyond the scope of this document. Any interested reader should refer to a good cryptography text for more information, such as Bruce Schneier's *Applied Cryptography*.

[Top of the section](#) [Close Section](#)

▣ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

[Top of the section](#) [Close Section](#)

▣ Workarounds

There is no configuration workaround.

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

[Top of the section](#) [Close Section](#)

☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

[Top of the section](#) [Close Section](#)

☐ **Customers using Third-party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#) [Close Section](#)

☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance

Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

Cisco has had no reports of malicious exploitation of this vulnerability.

Cisco knows of no public announcements of this vulnerability before the date of this notice. This vulnerability was discovered by an engineering analysis conducted by a Cisco customer at a security incident response organization.

[Top of the section](#) [Close Section](#)

☐ **Status of This Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-19980603-pix-key.shtml>. In addition to Worldwide Web posting, the initial version of this notice is being sent to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- firewalls@lists.gnac.net
- comp.security.firewalls
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

☐ Revision History

Revision 1.1	1998- June-16	Update to reflect change in plan; ECB mode being changed to CBC.
Revision 1.0	1998- June-03	Initial released version

[Top of the section](#) [Close Section](#)

☐ Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to security-alert@cisco.com. Reports may be encrypted using PGP; public RSA and DSS keys for "security-alert@cisco.com" are on the public PGP keyservers.

The alias "security-alert@cisco.com" is used only for reports incoming to Cisco. Mail sent to the list goes only to a very small group of users within Cisco. Neither outside users nor unauthorized Cisco employees may subscribe to "security-alert@cisco.com".

Please do not use "security-alert@cisco.com" for configuration questions, for security intrusions that you do not consider to be sensitive emergencies, or for general, non-security-related support requests. We do not have the capacity to handle such requests through this channel, and will refer them to the TAC, delaying response to your questions. We advise contacting the TAC directly with these requests. TAC contact numbers are as follows:

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

All formal public security notices generated by Cisco are sent to the public mailing list "cust-security-announce@cisco.com". For information on subscribing to this mailing list, send a message containing the single line "info cust-security-announce" to "majordomo@cisco.com". An analogous list, "cust-security-discuss@cisco.com" is available for public discussion of the notices and of other Cisco security issues. This notice is copyright 1998 by Cisco Systems, Inc.

This notice may be redistributed freely after the release date given at the top of the notice, provided that redistributed copies are complete and unmodified, including all date and version information.

[Top of the section](#) [Close Section](#)

Help us help you.

Please rate this document.

- Excellent
 Good
 Average
 Fair
 Poor

This document solved my problem.

- Yes
 No
 Just browsing

Suggestions for improvement:

(256 character limit)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

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