

Cisco Security Advisory: Vulnerabilities in Kerberos 5 Implementation

Document ID: 61720

Advisory ID: cisco-sa-20040831-krb5

<http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml>

Revision 1.0

For Public Release 2004 August 31 1830 UTC (GMT)

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

[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

Two vulnerabilities in the [Massachusetts Institute of Technology \(MIT\) Kerberos 5](#) implementation that affect Cisco VPN 3000 Series Concentrators have been announced by the MIT Kerberos Team.

Cisco VPN 3000 Series Concentrators authenticating users against a Kerberos Key Distribution Center (KDC) may be vulnerable to remote code execution and to Denial of Service (DoS) attacks. Cisco has made free software available to address these problems.

Cisco VPN 3000 Series Concentrators not authenticating users against a Kerberos Key Distribution Center (KDC) are not impacted.

No exploitations of these vulnerabilities have been reported.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following products have their Kerberos 5 implementation based on MIT Kerberos code and are affected by these vulnerabilities:

- Cisco VPN 3000 Series Concentrators. All 4.0.x software versions prior to 4.0.5.B and all 4.1.x software versions prior to 4.1.5.B are vulnerable. Versions prior to 4.0.x are **not vulnerable** since they do not support Kerberos authentication.

Note that vulnerable products are impacted **only** if they are configured to authenticate users against a Kerberos KDC.

Products Confirmed Not Vulnerable

The following products have Kerberos 5 support, but their implementation is not based on MIT Kerberos, and therefore are **not affected** by the vulnerabilities discussed in this advisory:

- Cisco IOS[®] (Kerberos support available in release 11.2 or later)
- Cisco CatOS

The following products do not have Kerberos 5 support and therefore are not affected by these vulnerabilities:

- Cisco PIX Firewall
- Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers

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

Details

Kerberos is a secret–key network authentication protocol developed at the Massachusetts Institute of Technology (MIT) that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos, like other secret–key systems, is based on the concept of a trusted third party that performs secure verification of users and services. In the Kerberos protocol, this trusted third party is called the Key Distribution Center (KDC).

The primary use of Kerberos is to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username–and–password authentication mechanism.

The Kerberos credential scheme embodies a concept called "single logon." This process requires authenticating a user once, and then allows secure authentication (without encrypting another password) wherever that user's credential is accepted.

Vulnerable Cisco devices using versions of Kerberos based on the MIT implementation to authenticate users are affected by two vulnerabilities. The first vulnerability consists of a double–free error that can happen under certain error conditions, and that can potentially allow a remote attacker to execute arbitrary code.

The second vulnerability consists of an infinite loop in the Abstract Syntax Notation (ASN) 1 decoder that can be entered upon receipt of an ASN.1 SEQUENCE type with invalid Basic Encoding Rules (BER) encoding. This vulnerability can be exploited by an attacker impersonating a legitimate Kerberos KDC or application server to cause a client program to hang inside an infinite loop, and thus creating a Denial of Service

condition. This vulnerability can also be exploited to cause a KDC or application server to hang inside an infinite loop.

More information about these MIT Kerberos vulnerabilities is available at <http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2004-002-dblfree.txt> and <http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2004-003-asn1.txt>. The information in these links is provided by MIT.

The two vulnerabilities described above are documented for the **Cisco VPN 3000 Series Concentrators** in Bug IDs [CSCef24692](#) ([registered](#) customers only) ([registered](#) customers only) and [CSCef24900](#) ([registered](#) customers only) ([registered](#) customers only).

Impact

An exploitation of the double-free vulnerability could potentially give an attacker control of the Cisco device and potentially compromise an entire Kerberos realm.

An exploitation of the "infinite loop in the ASN.1 decoder" vulnerability could potentially take out of service an affected product. The vulnerability could potentially be repeatedly exploited to keep the product out of service until an upgrade can be performed.

Software Versions and Fixes

The vulnerabilities described in this advisory are fixed in software versions 4.0.5.B and later and 4.1.5.B and later of the **Cisco VPN 3000 Series Concentrators**. If you are currently running the identified vulnerable software, you should obtain fixed software, as detailed below.

Workarounds

There is no workaround available to mitigate the effects of this vulnerability. Affected users should upgrade to a fixed version of the affected software.

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.

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>.

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.

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.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any malicious exploitation of the vulnerabilities described in this advisory.

These vulnerabilities were reported by the MIT Kerberos Team in concert with the CERT Coordination Center.

These vulnerabilities may impact other products that are not provided by Cisco. CERT/CC is coordinating the public disclosure of the impact these vulnerabilities may have on other, non-Cisco products. This Cisco Security Advisory is being published in coordination with CERT/CC.

The MIT Kerberos Team advisories for these vulnerabilities can be found at <http://web.mit.edu/kerberos/www/advisories/> (MITKRB5-SA-2004-002 and MITKRB5-SA-2004-003).

The CERT/CC advisories for these vulnerabilities can be found at <http://www.cert.org/advisories/>.

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.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com

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.

Revision History

Revision 1.0	2004 August 31	Initial public release.
--------------	----------------	-------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Aug 31, 2004

Document ID: 61720
