

[NEWS] Cisco VPN 3000 Kerberos Authentication Implementation Remote Code Execution And DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0011.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/02/04

To: list@securiteam.com

Date: 2 Sep 2004 14:19:10 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cisco VPN 3000 Kerberos Authentication Implementation Remote Code Execution And DoS

SUMMARY

<<http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/>> The Cisco VPN 3000 Series Concentrators are "purpose-built, remote access virtual private network (VPN) platforms that incorporate high availability, high performance, and scalability with the most advanced encryption and authentication techniques available today. Supported connectivity mechanisms include IP security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) over IPSec, and Cisco WebVPN (clientless secure sockets layer [SSL] browser-based connectivity)."

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.

DETAILS

Vulnerable Systems:

* Cisco VPN 3000 Series Concentrators versions 4.0.x, all versions prior to 4.0.5.B

Securiteam: [NEWS] Cisco VPN 3000 Kerberos Authentication Implementation Remote Code Execution And DoS

- * Cisco VPN 3000 Series Concentrators versions 4.1.x all versions prior to 4.1.5.B

Immune Systems:

- * Cisco IOS (Kerberos support available in release 11.2 or later)
- * Cisco CatOS
- * Cisco PIX Firewall (no Kerberos 5 support)
- * Cisco Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Series and Cisco 7600 Series routers (no Kerberos 5 support)

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

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. An attacker impersonating a legitimate Kerberos KDC or application server to cause a client program to hang inside an infinite loop, thus creating a Denial of Service condition, can exploit this vulnerability. This vulnerability can also be exploited to cause a KDC or application server to hang inside an infinite loop.

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.

Vendor Status:

Cisco has already released updated software revisions for the affected devices that fix the abovementioned vulnerabilities.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

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

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.