

www.ncp.de

Vulnerability Issues in Implementation of ISAKMP Protocol

VPN products from a variety of vendors, including Cisco and Juniper, are vulnerable to a denial-of-service attack, thanks to a flaw that was recently discovered by researchers at Finland's University of Oulu.

NCP Secure Communications products are not impacted by the ISAKMP vulnerability.

Nov. 14, 2005. The British National Infrastructure Security Co-ordination Centre and the Finnish CERT published a joint vulnerability advisory "Multiple Vulnerability Issues in Implementation of ISAKMP Protocol".

"The flaw affects a component of the IPSec protocol used by VPN software and hardware to securely exchange data over the Internet. While there is some risk of affected VPN systems being taken over by attackers, a more likely threat is a denial-of-service attack, in which machines would be forced to reset repeatedly, jamming up networks and causing headaches for users." (Robert McMillan, IDG News Service)

About ISAKMP

The vulnerabilities described in this advisory affect the Internet Security Association and Key Management Protocol (ISAKMP), which is used to provide associations for other security protocols. ISAKMP is an important part of the IPSec negotiations, which is widely used to securely exchange packets at the IP layer and mostly used to implement Virtual Private Networks (VPNs). Since IPSec encrypts packets and creates secure tunnels for traffic traveling over the public Internet and into corporate network environments, ISAKMP plays a key role in helping remote access users securely connect to their company's corporate networks.

The ISAKMP has a complicated message design. An ISAKMP message is made up by a message header and one or more payloads, which could be, e.g., proposal, certificate, hash, or signature. The contents of the payloads as well as the length fields may possibly be manipulated. It is also possible to create a proposal list with a lot of proposals, which may cause trouble for the recipient.

NCP's Commentary

The problems described in the advisory do not affect the security of the ISAKMP handshakes. ISAKMP is probably the most investigated security protocol around. The flaws are related to denial-of-service (DoS) and not to the basic ISAKMP key exchanges and authentication.

The advisory recommends to avoid the use of Aggressive Mode in Phase 1 because of potential DoS problems. However, Aggressive Mode in Phase 1 contains fewer messages with more payload within the messages. The problem lies within the parsing of the received messages. Either the parsing is executed correctly or not. The vulnerability of ISAKMP depends on its vendor-specific implementation.

NCP's Product Statement

The advisory states that the vulnerability's severity varies according to the vendor-specific implementation and is restricted to servers. The IKE/IPSec implementation of both, NCP Secure Enterprise Servers and NCP Secure Clients have passed extensive penetration tests by independent specialists and trusted companies.

NCP reports that NCP Secure Communications products are not affected by this vulnerability even though NCP Secure Clients use ISAKMP to communicate with NCP Secure Enterprise Servers or IPSec gateways from other vendors.

NCP does not warrant that IPSec gateways from other vendors cannot be impacted by the ISAKMP vulnerability. NCP customers using non-NCP gateways should consult the VPN gateway provider.

NCP has a large installed base of NCP Secure Clients with features that allow clients to seamlessly interoperate with NCP Secure Enterprise Servers or other VPN gateways for effective IPSec-protected secure remote access.