CVE-2006-3551

Published on: 07/12/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-3551

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

Certain versions of Secure Client from Ncp Network Communications contain the following vulnerability:

NCP Secure Enterprise Client (aka VPN/PKI client) 8.30 Build 59, and possibly earlier versions, when the Link Firewall and Personal Firewall are both configured to block all inbound and outbound network traffic, allows context-dependent attackers to send inbound UDP traffic with source port 67 and destination port 68, and outbound UDP traffic with source port 68 and destination port 67.

CVE-2006-3551 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 1.2 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[Full-disclosure] NCP VPN/PKI Client: UDP Bypassing	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060630 NCP VPN/PKI Client: UDP Bypassing
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ncp-vpnpki-udp-bypass-security(27484)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ncp Network Communications	Secure Client	All	All	All	All

cpe:2.3:a:ncp_network_communications:secure_client:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→