



# CVE-2006-0967

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2006-0967                                                                                                           |
| State           | PUBLISHED                                                                                                               |
| Assigner        | mitre                                                                                                                   |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                            |
| Published       | 2006-03-02 23:02:00 UTC                                                                                                 |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                 |
| Description     | NCP Network Communication Secure Client 8.11 Build 146, and possibly other versions, allows local users to cause a deni |

## Risk And Classification

**Primary CVSS:** v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:N/I:N/A:P

**EPSS:** 0.000720000 probability, percentile 0.220070000 (date 2026-04-16)

**Problem Types:** CWE-399 | n/a

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:L/AC:L/Au:N/C:N/I:N/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------|--------|---------|---------|--------|---------|----------|
|------|--------|---------|---------|--------|---------|----------|

|                                                                               |                                      |               |                |                                                                                 |     |     |
|-------------------------------------------------------------------------------|--------------------------------------|---------------|----------------|---------------------------------------------------------------------------------|-----|-----|
| Application                                                                   | Ncp Network Communications           | Secure Client | 8.11_build_146 | All                                                                             | All | All |
| Vendor Declared Affected Products                                             |                                      |               |                |                                                                                 |     |     |
| Source                                                                        | Vendor                               | Product       | Version        | Platforms                                                                       |     |     |
| CNA                                                                           | Na                                   | N/a           | affected n/a   | Not specified                                                                   |     |     |
| References                                                                    |                                      |               |                |                                                                                 |     |     |
| Reference                                                                     | Source                               |               |                | Link                                                                            |     |     |
| Secunia - Advisories - NCP Secure Entry/Enterprise Client Two Vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 |               |                | <a href="https://secunia.com">secunia.com</a>                                   |     |     |
| NCP Secure Client Multiple Vulnerabilities                                    | af854a3a-2127-422b-91ae-364da2661108 |               |                | <a href="https://www.securityfocus.com">www.securityfocus.com</a>               |     |     |
| SecurityFocus                                                                 | af854a3a-2127-422b-91ae-364da2661108 |               |                | <a href="https://www.securityfocus.com">www.securityfocus.com</a>               |     |     |
| [Full-disclosure] NCP VPN/PKI Client - various Bugs                           | af854a3a-2127-422b-91ae-364da2661108 |               |                | <a href="https://lists.grok.org.uk">lists.grok.org.uk</a>                       |     |     |
| IBM X-Force Exchange                                                          | af854a3a-2127-422b-91ae-364da2661108 |               |                | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |     |     |
| CVE Program record                                                            | CVE.ORG                              |               |                | <a href="https://www.cve.org">www.cve.org</a>                                   |     |     |
| NVD vulnerability detail                                                      | NVD                                  |               |                | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                                 |     |     |
| No vendor comments have been submitted for this CVE.                          |                                      |               |                |                                                                                 |     |     |
| There are currently no legacy QID mappings associated with this CVE.          |                                      |               |                |                                                                                 |     |     |