



# CVE-2004-0365

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2004-0365                                                                                                                |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2004-05-04 04:00:00 UTC                                                                                                      |
| <b>Updated</b>         | 2023-12-28 15:33:00 UTC                                                                                                      |
| <b>Description</b>     | The dissect_attribute_value_pairs function in packet-radius.c for Ethereal 0.8.13 to 0.10.2 allows remote attackers to cause |

## Risk And Classification

### Problem Types: CWE-476

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                         | Product                  | Version | Update | Edition | Language |
|-------------|--------------------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Ethereal</a>       | <a href="#">Ethereal</a> | All     | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.10    | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.10.1  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.10.2  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.13  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.14  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.18  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.19  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9     | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.1   | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.10  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.11  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.12  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.13  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.14  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.15  | All    | All     | All      |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.16  | All    | All     | All      |

|             |                                |                          |        |     |     |     |
|-------------|--------------------------------|--------------------------|--------|-----|-----|-----|
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.2  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.3  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.4  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.5  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.6  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.7  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.8  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.9  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.10   | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.10.1 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.10.2 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.13 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.14 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.18 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.8.19 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9    | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.1  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.10 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.11 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.12 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.13 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.14 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.15 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.16 | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.2  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.3  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.4  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.5  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.6  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.7  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.8  | All | All | All |
| Application | <a href="#">Ethereal Group</a> | <a href="#">Ethereal</a> | 0.9.9  | All | All | All |

| References          |  |  |  |        |            |   |
|---------------------|--|--|--|--------|------------|---|
| Reference           |  |  |  | Source | Link       | T |
| Blockchain (C) 2018 |  |  |  | Q&A    | Blockchain |   |

|                                                                                         |           |                                                                                 |   |
|-----------------------------------------------------------------------------------------|-----------|---------------------------------------------------------------------------------|---|
| Repository / Oval Repository                                                            | OVAL      | <a href="https://oval.cisecurity.org">oval.cisecurity.org</a>                   |   |
| redhat.com   Red Hat Support                                                            | REDHAT    | <a href="https://www.redhat.com">www.redhat.com</a>                             |   |
| Home - Conectiva                                                                        | CONECTIVA | <a href="https://distro.conectiva.com.br">distro.conectiva.com.br</a>           |   |
| Ethereal: enpa-sa-00013                                                                 | CONFIRM   | <a href="https://www.ethereal.com">www.ethereal.com</a>                         |   |
| '[OpenPKG-SA-2004.015] OpenPKG Security Advisory (ethereal)' - MARC                     | BUGTRAQ   | <a href="https://marc.info">marc.info</a>                                       |   |
| US-CERT Vulnerability Note VU#124454                                                    | CERT-VN   | <a href="https://www.kb.cert.org">www.kb.cert.org</a>                           | U |
| Repository / Oval Repository                                                            | OVAL      | <a href="https://oval.cisecurity.org">oval.cisecurity.org</a>                   |   |
| '[Ethereal-dev] ethereal radius dissector vulnerability' - MARC                         | MLIST     | <a href="https://marc.info">marc.info</a>                                       |   |
| 'LNSA-#2004-0007: Multiple security problems in Ethereal' - MARC                        | BUGTRAQ   | <a href="https://marc.info">marc.info</a>                                       |   |
| Gentoo Linux Documentation -- Multiple remote overflows and vulnerabilities in Ethereal | GENTOO    | <a href="https://security.gentoo.org">security.gentoo.org</a>                   | V |
| Secunia - Advisories - Ethereal Multiple Vulnerabilities                                | SECUNIA   | <a href="https://secunia.com">secunia.com</a>                                   |   |
| Repository / Oval Repository                                                            | OVAL      | <a href="https://oval.cisecurity.org">oval.cisecurity.org</a>                   |   |
| IBM X-Force Exchange                                                                    | XF        | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |   |
| Mandriva Security Advisories                                                            | MANDRAKE  | <a href="https://www.mandriva.com">www.mandriva.com</a>                         |   |
| redhat.com   Red Hat Support                                                            | REDHAT    | <a href="https://www.redhat.com">www.redhat.com</a>                             |   |
| CVE Program record                                                                      | CVE.ORG   | <a href="https://www.cve.org">www.cve.org</a>                                   | c |
| NVD vulnerability detail                                                                | NVD       | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                                 | c |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)