



# CVE-2004-2194

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

## Summary

|                 |                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2004-2194                                                                                                                                                                      |
| State           | PUBLISHED                                                                                                                                                                          |
| Assigner        | mitre                                                                                                                                                                              |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                                                                       |
| Published       | 2004-12-31 05:00:00 UTC                                                                                                                                                            |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                                                                            |
| Description     | MailEnable Professional Edition before 1.53 and Enterprise Edition before 1.02 allows remote attackers to cause a denial of service (CPU consumption) via a crafted email message. |

## Risk And Classification

**Primary CVSS:** v2.0 5 from nvd@nist.gov

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

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/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 | Mailenable | Mailenable Enterprise | 1.0     | All    | All     | All      |

|             |                            |                                         |      |     |     |     |
|-------------|----------------------------|-----------------------------------------|------|-----|-----|-----|
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Enterprise</a>   | 1.00 | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Enterprise</a>   | 1.01 | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Enterprise</a>   | All  | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.17 | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.18 | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.19 | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.2  | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.2a | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.5  | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.51 | All | All | All |
| Application | <a href="#">Mailenable</a> | <a href="#">Mailenable Professional</a> | 1.52 | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |

| References                                                   |                                      |                                       |       |  |
|--------------------------------------------------------------|--------------------------------------|---------------------------------------|-------|--|
| Reference                                                    | Source                               | Link                                  | Tags  |  |
| MailEnable Multiple Remote Denial Of Service Vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.securityfocus.com</a> |       |  |
| MailEnable - Enterprise Edition Revision History             | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.mailenable.com</a>    | Patch |  |
| MailEnable - Professional Edition Revision History           | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">www.mailenable.com</a>    | Patch |  |
| CVE Program record                                           | CVE.ORG                              | <a href="#">www.cve.org</a>           | canon |  |
| NVD vulnerability detail                                     | NVD                                  | <a href="#">nvd.nist.gov</a>          | canon |  |

No vendor comments have been submitted for this CVE.

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