



# CVE-2014-9376

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2014-9376
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-12-19 15:59:27 UTC
<b>Updated</b>	2026-05-06 22:30:45 UTC
<b>Description</b>	Integer underflow in Ettercap 0.8.1 allows remote attackers to cause a denial of service (out-of-bounds write) and possibly e

## Risk And Classification

**Primary CVSS:** v2.0 7.5 from nvd@nist.gov

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

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ettercap-project	Ettercap	0.8.1	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

## References

Reference	Source
Fix arbitrary length by NickSampanis · Pull Request #602 · Ettercap/ettercap · GitHub	af854a3a-2127-422b-91ae
Ettercap 'dissector_dhcp()' Function Denial of Service Vulnerability	af854a3a-2127-422b-91ae
SecurityFocus	af854a3a-2127-422b-91ae
Fix gg dissector arbitrary length heap overflow by NickSampanis · Pull Request #606 · Ettercap/ettercap · GitHub	af854a3a-2127-422b-91ae
Obrela - Obrela Security	af854a3a-2127-422b-91ae
Ettercap: Multiple vulnerabilities (GLSA 201505-01) — Gentoo security	af854a3a-2127-422b-91ae
Fix cvs signed pointer by NickSampanis · Pull Request #609 · Ettercap/ettercap · GitHub	af854a3a-2127-422b-91ae
Fix TN3270 out of bounds write by NickSampanis · Pull Request #605 · Ettercap/ettercap · GitHub	af854a3a-2127-422b-91ae
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)