



CVE-2002-1355

Published on: 12/17/2002 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1355

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ethereal](#) from [Ethereal Group](#) contain the following vulnerability:

Multiple integer signedness errors in the BGP dissector in Ethereal 0.9.7 and earlier allow remote attackers to cause a denial of service (infinite loop) via malformed messages.

CVE-2002-1355 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Ethereal: enpa-sa-00007

[Patch](#)
[Vendor Advisory](#)
[www.ethereal.com](#)
[text/html](#)

[CONFIRM www.ethereal.com/apnotes/enpa-sa-00007.html](#)

AOS Cloud Services - Backup and
Storage Solutions

[www.ethereal.com](#)
[text/html](#)

[CONFIRM www.ethereal.com/cgi-bin/viewcvs.cgi/ethereal/packet-bgp.c.diff?r1=1.68&r2=1.69](#)

redhat.com | Red Hat Support

[Patch](#)
[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2002:290](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

CVE.report does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ethereal Group	Ethereal	All	All	All	All
cpe:2.3:a:ethereal_group:ethereal:*.***.***.***:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)