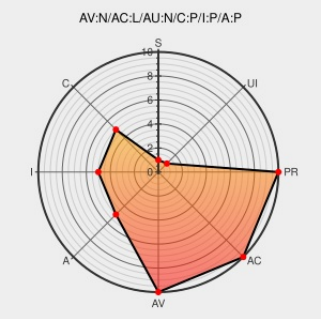
CVE-2002-1356

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

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

CVE-2002-1356

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ethereal from Ethereal Group contain the following vulnerability:

Ethereal 0.9.7 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed packets to the (1) LMP, (2) PPP, or (3) TDS dissectors, possibly related to a missing field for EndVerifyAck messages.

CVE-2002-1356 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Ethereal: enpa-sa-00007	Patch, Vendor Advisory, www.ethereal.com, text/html	CONFIRM www.ethereal.com/appnotes/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-lmp.c#rev1.13
redhat.com | Red Hat Support	Patch, Vendor Advisory, www.redhat.com, text/html	REDHAT RHSA-2002:290

CVEreport 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→