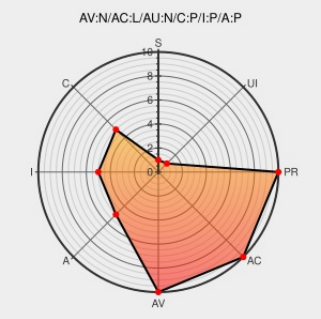
CVE-2005-2367

Published on: 08/10/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2005-2367

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



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

Format string vulnerability in the proto_item_set_text function in Ethereal 0.9.4 through 0.10.11, as used in multiple dissectors, allows remote attackers to write to arbitrary memory locations and gain privileges via a crafted AFP packet.

CVE-2005-2367 has been assigned by secalert@redhat.com 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
Secunia - Advisories - Debian update for ethereal	web.archive.org, text/html	SECUNIA 17102
Secunia - Advisories - Ethereal Multiple Protocol Dissector and zlib Vulnerabilities	web.archive.org, text/html	SECUNIA 16225
Gentoo Linux Documentation -- Ethereal: Multiple vulnerabilities	Patch, www.gentoo.org, text/html	GENTOO GLSA-200507-27
Advisories - Mandriva	Patch, Vendor Advisory, www.mandriva.com, text/html	MANDRAKE MDKSA-2005:131
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:10765

Ethereal Multiple Protocol Dissector Vulnerabilities	cve.report (archive) text/html	BID 14399
Accenture | Let there be change	Vendor Advisory www.idefense.com text/html	IDEFENSE 20050805 Multiple Vendor Ethereal AFP Protocol Dissector Format String Vulnerability
Debian -- Security Information -- DSA-853-1 ethereal	www.debian.org Depreciated Link text/html	DEBIAN DSA-853
[FLSA-2006:152922] Updated ethereal packages fix security issues	www.redhat.com text/html	FEDORA FLSA-2006:152922
Ethereal: enpa-sa-00020	Patch www.ethereal.com text/xml	CONFIRM www.ethereal.com/appnotes/enpa-sa-00020.html
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2005:687
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:019
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:018

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	0.10.0	All	All	All
Application	Ethereal Group	Ethereal	0.10.1	All	All	All
Application	Ethereal Group	Ethereal	0.10.10	All	All	All
Application	Ethereal Group	Ethereal	0.10.11	All	All	All
Application	Ethereal Group	Ethereal	0.10.2	All	All	All
Application	Ethereal Group	Ethereal	0.10.3	All	All	All
Application	Ethereal Group	Ethereal	0.10.4	All	All	All
Application	Ethereal Group	Ethereal	0.10.5	All	All	All
Application	Ethereal Group	Ethereal	0.10.6	All	All	All
Application	Ethereal Group	Ethereal	0.10.7	All	All	All
Application	Ethereal Group	Ethereal	0.10.8	All	All	All
Application	Ethereal Group	Ethereal	0.10.9	All	All	All

Application	Ethereal Group	Ethereal	0.9.10	All	All	All
Application	Ethereal Group	Ethereal	0.9.11	All	All	All
Application	Ethereal Group	Ethereal	0.9.12	All	All	All
Application	Ethereal Group	Ethereal	0.9.13	All	All	All
Application	Ethereal Group	Ethereal	0.9.14	All	All	All
Application	Ethereal Group	Ethereal	0.9.15	All	All	All
Application	Ethereal Group	Ethereal	0.9.16	All	All	All
Application	Ethereal Group	Ethereal	0.9.4	All	All	All
Application	Ethereal Group	Ethereal	0.9.5	All	All	All
Application	Ethereal Group	Ethereal	0.9.6	All	All	All
Application	Ethereal Group	Ethereal	0.9.7	All	All	All
Application	Ethereal Group	Ethereal	0.9.8	All	All	All
Application	Ethereal Group	Ethereal	0.9.9	All	All	All
Application	Ethereal Group	Ethereal	0.10.0	All	All	All
Application	Ethereal Group	Ethereal	0.10.1	All	All	All
Application	Ethereal Group	Ethereal	0.10.10	All	All	All
Application	Ethereal Group	Ethereal	0.10.11	All	All	All
Application	Ethereal Group	Ethereal	0.10.2	All	All	All
Application	Ethereal Group	Ethereal	0.10.3	All	All	All
Application	Ethereal Group	Ethereal	0.10.4	All	All	All
Application	Ethereal Group	Ethereal	0.10.5	All	All	All
Application	Ethereal Group	Ethereal	0.10.6	All	All	All
Application	Ethereal Group	Ethereal	0.10.7	All	All	All
Application	Ethereal Group	Ethereal	0.10.8	All	All	All
Application	Ethereal Group	Ethereal	0.10.9	All	All	All
Application	Ethereal Group	Ethereal	0.9.10	All	All	All
Application	Ethereal Group	Ethereal	0.9.11	All	All	All
Application	Ethereal Group	Ethereal	0.9.12	All	All	All
Application	Ethereal Group	Ethereal	0.9.13	All	All	All
Application	Ethereal Group	Ethereal	0.9.14	All	All	All
Application	Ethereal Group	Ethereal	0.9.15	All	All	All
Application	Ethereal Group	Ethereal	0.9.16	All	All	All
Application	Ethereal Group	Ethereal	0.9.4	All	All	All
Application	Ethereal Group	Ethereal	0.9.5	All	All	All
Application	Ethereal Group	Ethereal	0.9.6	All	All	All
Application	Ethereal Group	Ethereal	0.9.7	All	All	All

Application	Ethereal Group	Ethereal	0.9.8	All	All	All
Application	Ethereal Group	Ethereal	0.9.9	All	All	All

- cpe:2.3:a:ethereal_group:ethereal:0.10.0:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.1:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.10:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.11:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.2:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.3:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.4:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.5:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.6:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.7:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.8:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.9:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.10:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.11:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.12:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.13:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.14:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.15:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.16:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.4:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.5:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.6:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.7:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.8:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.9.9:*:*:*:*:*:*:*
- cpe:2.3:a:ethereal_group:ethereal:0.10.0:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.1:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.10:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.11:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.2:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.3:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.4:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.5:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.6:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.7:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.8:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.10.9:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.10:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.11:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.12:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.13:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.14:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.15:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.16:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.4:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.5:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.6:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.7:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.8:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report