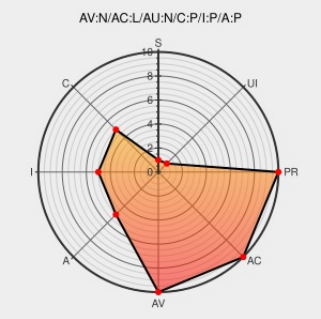
CVE-2003-0927

Published on: 11/06/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:46 PM UTC

CVE-2003-0927

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



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

Heap-based buffer overflow in Ethereal 0.9.15 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the SOCKS dissector.

CVE-2003-0927 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
Mandriva Security Advisories	www.mandriva.com text/html	MANDRAKE MDKSA-2003:114
404 Not Found	www.turbolinux.com text/plain Inactive Link Not Archived	TURBO TLSA-2003-64
Ethereal: enpa-sa-00011	Patch Vendor Advisory www.ethereal.com text/html	CONFIRM www.ethereal.com/appnotes/enpa-sa-00011.html
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ethereal-socks-heap-overflow(13578)
redhat.com | Red Hat Support	Patch Vendor Advisory	REDHAT RHSA-2003:323

	www.redhat.com text/html	
Secunia - Advisories - Debian update for ethereal	web.archive.org text/html	SECUNIA 10531
Debian -- Page not found	www.debian.org Depreciated Link text/html Inactive Link Not Archived	DEBIAN DSA-407
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9691
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:324
Home - Conectiva	distro.conectiva.com.br text/html	CONECTIVA CLA-2003:780
Multiple Ethereal Protocol Dissector Vulnerabilities	Patch Vendor Advisory cve.report (archive) text/html	BID 8951

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	0.9	All	All	All
Application	Ethereal Group	Ethereal	0.9.1	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	0.9.2	All	All	All
Application	Ethereal Group	Ethereal	0.9.3	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	0.9	All	All	All
Application	Ethereal Group	Ethereal	0.9.1	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	0.9.2	All	All	All
Application	Ethereal Group	Ethereal	0.9.3	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:0.9:*:*:*:*:*:*:*:

cpe:2.3:a:ethereal_group:ethereal:0.9.1:*:*:*:*:*:*:*:

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:0.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:ethereal_group:ethereal:0.9.3:*:*:*:*:*:*:*:

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:0.9.8:*:*:*:*:*:*:*

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

cpe:2.3:a:ethereal_group:ethereal:0.9:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.1:*:*:*:*:*:*:*

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:0.9.2:*:*:*:*:*:*:*

cpe:2.3:a:ethereal_group:ethereal:0.9.3:*:*:*:*:*:*:*

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→