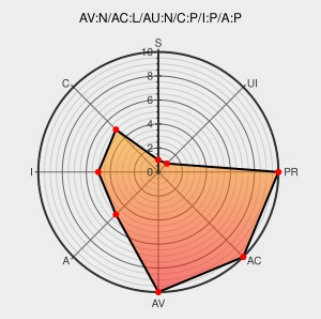
CVE-2003-0081

Published on: 03/18/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-0081

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



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

Format string vulnerability in packet-socks.c of the SOCKS dissector for Ethereal 0.8.7 through 0.9.9 allows remote attackers to execute arbitrary code via SOCKS packets containing format string specifiers.

CVE-2003-0081 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
NOVELL: Broken Link - 404 Error Pages	web.archive.org text/html Inactive Link Not Archived	SUSE SuSE-SA:2003:019
Ethereal: enpa-sa-00008	Patch Vendor Advisory www.ethereal.com text/html	CONFIRM www.ethereal.com/appnotes/enpa-sa-00008.html
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ethereal-socks-format-string(11497)
LinuxSecurity.com: Gentoo: ethereal Arbitrary code execution	www.linuxsecurity.com text/html	GENTOO GLSA-200303-10
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:077

Debian -- Security Information -- DSA-258-1 ethereal	Patch Vendor Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-258
Home - Conectiva	distro.conectiva.com.br text/html	CONECTIVA CLSA-2003:627
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:54
FullDisclosure: Ethereal format string bug, yet still ethereal much better than windows	seclists.org text/html	FULLDISC 20030308 Ethereal format string bug, yet still ethereal much better than windows
Ethereal format string bug, yet still ethereal much better than windows	Exploit Patch Vendor Advisory www.guninski.com text/html	MISC www.guninski.com/etherre.html
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:076
Ethereal SOCKS Dissector Format String Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	BID 7049
frontal2.mandriva.com	frontal2.mandriva.com text/html	MANDRAKE MDKSA-2003:051

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	0.8.18	All	All	All
Application	Ethereal Group	Ethereal	0.9.0	All	All	All
Application	Ethereal Group	Ethereal	0.9.1	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	0.8.18	All	All	All
Application	Ethereal Group	Ethereal	0.9.0	All	All	All
Application	Ethereal Group	Ethereal	0.9.1	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:0.8.18:*:*:*:*:*:*:*:

cpe:2.3:a:ethereal_group:ethereal:0.9.0:*:*:*:*:*:*:*:

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

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:*:*:*:*:*:*:*:

cpe:2.3:a:ethereal_group:ethereal:0.8.18:*:*:*:*:*:*:*:

cpe:2.3:a:ethereal_group:ethereal:0.9.0:*:*:*:*:*:*:*:

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

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→