

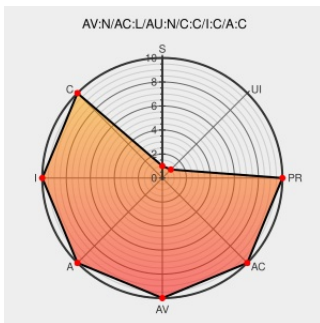


CVE-2005-3184

Published on: 10/20/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

CVE-2005-3184

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

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

Buffer overflow vulnerability in the unicode_to_bytes in the Service Location Protocol (srvloc) dissector (packet-srvloc.c) in Ethereal allows remote attackers to execute arbitrary code via a srvloc packet with a modified length value.

CVE-2005-3184 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Accenture | Let there be change

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

[IDEFENSE 20051020 Multiple Vendor Ethereal srvloc Buffer Overflow Vulnerability](#)

Secunia - Advisories - Gentoo update for ethereal

[web.archive.org](#)
[text/html](#)

[SECUNIA 17377](#)

Secunia - Advisories - Red Hat update for ethereal

[web.archive.org](#)
[text/html](#)

[SECUNIA 17327](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL](#)
[oval.org.mitre.oval:def:10074](#)

[rhn.redhat.com](#) | Red Hat Support

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

[REDHAT RHSA-2005:809](#)

No Description Provided	www.osvdb.org	OSVDB 20137
	Inactive Link Not Archived	
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:025
Secunia - Advisories - Ethereum Multiple Protocol Dissector and PCRE Vulnerabilities	web.archive.org text/html	SECUNIA 17254
Secunia - Advisories - Avaya Multiple Ethereum Vulnerabilities	web.archive.org text/html	SECUNIA 17392
Ethereal: enpa-sa-00021	www.ethereal.com text/xml	CONFIRM www.ethereal.com/appnotes/enpa-sa-00021.html
Gentoo Linux Documentation -- Ethereum: Multiple vulnerabilities in protocol dissectors	www.gentoo.org text/html	GENTOO GLSA-200510-25
[FLSA-2006:152922] Updated ethereal packages fix security issues	www.redhat.com text/html	FEDORA FLSA-2006:152922
SecurityTracker.com Archives - Ethereum Bugs in Multiple Dissectors Let Remote Users Execute Arbitrary Code or Cause Denial of Service Conditions	securitytracker.com text/html	SECTrack 1015082
Ethereal Multiple Protocol Dissector Vulnerabilities In Versions Prior To 0.10.13	cve.report (archive) text/html	BID 15148
Ethereal Service Location Protocol Dissection Stack Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 15158
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	SECUNIA 17480
Secunia - Advisories - Fedora update for ethereal	web.archive.org text/html	SECUNIA 17286

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 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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)