CVE-2005-0739

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2005-0739
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The IAPP dissector (packet-iapp.c) for Ethereal 0.9.1 to 0.10.9 does not properly use certain routines for formatting strings,

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ethereal Group	Ethereal	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Ethereal - This Ultra Rare Brand Concept is Available for Purchase.	af854a3a-2127-422b-91ae-364da2661108	anonsvn.ethereal.com
Gentoo Linux Documentation -- Ethereal: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.gentoo.org
Ethereal Etheric/GPRS-LLC/IAPP/JXTA/sFlow Dissector Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.cor
rhn.redhat.com | Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
Advisories - Mandriva	af854a3a-2127-422b-91ae-364da2661108	www.mandriva.com
[FLSA-2006:152922] Updated ethereal packages fix security issues	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
'Ethereal remote buffer overflow #2' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
Debian -- Security Information -- DSA-718-2 ethereal	af854a3a-2127-422b-91ae-364da2661108	www.debian.org
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org
404 Not Found	af854a3a-2127-422b-91ae-364da2661108	security.lss.hr
Ethereal: enpa-sa-00018	af854a3a-2127-422b-91ae-364da2661108	www.ethereal.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.