CVE-2005-1796

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

Summary

CVE	CVE-2005-1796
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-31 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Format string vulnerability in the curses_msg function in the Ncurses interface (ec_curses.c) for Ettercap before 0.7.3 allow

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	3.0	All	All	All

Operating System	Debian	Debian Linux	3.1	All	All	All
Application	Ettercap	Ettercap	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
SecurityTracker.com Archives - Ettercap Format String Flaw in curses_msg() Lets Remote Users Execute Arbitrary Code	af854a3a-2127-42
Gentoo Linux Documentation -- Ettercap: Format string vulnerability	af854a3a-2127-42
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-42
Secunia - Advisories - Ettercap "curses_msg()" Format String Vulnerability	af854a3a-2127-42
Secunia - Advisories - Debian update for ettercap	af854a3a-2127-42
Secunia - Advisories - Gentoo update for ettercap	af854a3a-2127-42
Ettercap Remote Format String Vulnerability	af854a3a-2127-42
Debian -- Security Information -- DSA-749-1 ettercap	af854a3a-2127-42
ettercap	af854a3a-2127-42
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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