



CVE-2004-1210

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2004-1210
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-10 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cross-site scripting (XSS) vulnerability in proxylog.dat in IPCop 1.4.1 and possibly other versions, allows remote attackers to

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	lpcop	lpcop	1.4.1	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
IPCop Web Administration Interface Proxy Log HTML Injection Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.security
'[KA Advisory 0411291] IPCop Cross Site Scripting Vulnerability in' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xfo
[KA Advisory 0411291] IPCop Cross Site Scripting Vulnerability in "proxylog.dat"	af854a3a-2127-422b-91ae-364da2661108	www.kurczab
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.