CVE-2004-2416

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

Summary

CVE	CVE-2004-2416
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in the logging component of CCProxy allows remote attackers to execute arbitrary code via a long HTTP GE

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
Application	Youngzsoft	Ccproxy	6.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
'CCProxy Log Stack Overflow' - SecuriTeam	af854a3a-2127-4
IBM X-Force Exchange	af854a3a-2127-4
www.osvdb.org/11593	af854a3a-2127-4
Youngzsoft CCProxy Logging Function Unspecified Remote Buffer Overflow Vulnerability	af854a3a-2127-4
SecurityTracker.com Archives - CCProxy Buffer Overflow in Logging Function Lets Remote Users Execute Arbitrary Code	af854a3a-2127-4
Secunia - Advisories - CCProxy HTTP Request Processing Buffer Overflow Vulnerability	af854a3a-2127-4
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.