CVE-2006-0304

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

Summary

CVE	CVE-2006-0304
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-19 00:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in Dual DHCP DNS Server 1.0 allows remote attackers to cause a denial of service (application crash) and

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

EPSS: 0.165940000 probability, percentile 0.949290000 (date 2026-04-16)

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	Achal Dhir	Dual Dhcp Dns Server	1.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Dual DHCP DNS Server DHCP Options Buffer Overflow - Advisories - Secunia	af854a3a-2127-422b-9
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-9
Dual DHCP DNS Server DHCP Options Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-9
SecurityTracker.com Archives - Dual DHCP DNS Server Buffer Overflow Lets Remote Users Execute Arbitrary Code	af854a3a-2127-422b-9
IBM X-Force Exchange	af854a3a-2127-422b-9
aluigi.altervista.org/adv/dualsbof-adv.txt	af854a3a-2127-422b-9
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.