CVE-2011-0404

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

Summary

CVE	CVE-2011-0404
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-11 03:00:05 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in NetSupport Manager Agent for Linux 11.00, for Solaris 9.50, and for Mac OS X 11.00 allows

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: CWE-119 | 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	Netsupport	Netsupport Manager Agent	11.00	All	linux	All

Application	Netsupport	Netsupport Manager Agent	11.00	All	mac_os_x	All
Application	Netsupport	Netsupport Manager Agent	9.50	All	solaris	All

Vendor Declared Affected Products

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

References

Reference	Source
NEOHAPSIS - Peace of Mind Through Integrity and Insight	af854a3a-2127-422b-91ae-364da
404 Not Found	af854a3a-2127-422b-91ae-364da
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da
NetSupport Manager Remote Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da
NetSupport Manager Agent Stack Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da
osvdb.org/70408	af854a3a-2127-422b-91ae-364da
NetSupport Manager Client Buffer Overflow Vulnerability - Secunia.com	af854a3a-2127-422b-91ae-364da
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da
NetSupport Manager Agent Remote Buffer Overflow	af854a3a-2127-422b-91ae-364da
NetSupport Manager Agent Remote Buffer Overflow	af854a3a-2127-422b-91ae-364da
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.