CVE-2007-0355

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

Summary

CVE	CVE-2007-0355
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-19 01:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Buffer overflow in the Apple Minimal SLP v2 Service Agent (slpd) in Mac OS X 10.4.11 and earlier, including 10.4.8, allows

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	10.4.8	All	All	All

Application	Apple	Minimal Slp Service Agent	10.4.11	All	All	All

Vendor Declared Affected Products

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

References

Reference
SecurityTracker.com Archives - Apple Service Location Protocol Daemon (slpd) Buffer Overflow May Let Local Users Gain Elevated Privileges
About the security content of Mac OS X 10.5.2 and Security Update 2008-001
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
www.osvdb.org/32693
APPLE-SA-2008-02-11 Mac OS X v10.5.2 and Security Update 2008-001
IBM X-Force Exchange
US-CERT Technical Cyber Security Alert TA08-043B -- Apple Updates for Multiple Vulnerabilities
Mac OS X 10.4.8 SLP Daemon Service Registration Buffer Overflow PoC
Mac OS X Buffer Overflow in Directory Services Lets Local Users Execute Arbitrary Code - SecurityTracker
MOAB-17-01-2007: Apple SLP Daemon Service Registration Buffer Overflow Vulnerability
Apple Mac OS X slpd Buffer Overflow Vulnerability - Advisories - Secunia
Apple Mac OS X SLP Daemon Service Registration Local Buffer Overflow Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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