



CVE-2004-0824

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

Summary

CVE	CVE-2004-0824
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	PPPDialer for Mac OS X 10.2.8 through 10.3.5 allows local users to overwrite system files via a symlink attack on PPPDialer

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	10.2.8	All	All	All

Operating System	Apple	Mac Os X	10.3	All	All	All
Operating System	Apple	Mac Os X	10.3.1	All	All	All
Operating System	Apple	Mac Os X	10.3.2	All	All	All
Operating System	Apple	Mac Os X	10.3.3	All	All	All
Operating System	Apple	Mac Os X	10.3.4	All	All	All
Operating System	Apple	Mac Os X	10.3.5	All	All	All

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

References		
Reference	Source	L
O-212: Apple Security Update	af854a3a-2127-422b-91ae-364da2661108	w
Apple PPPDialer Insecure Log File Creation Symbolic Link Vulnerability	af854a3a-2127-422b-91ae-364da2661108	w
PPPDialer Unsafe Log Files May Let Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108	s
Advisory: Security Update 2004-09-07	af854a3a-2127-422b-91ae-364da2661108	w
AusCERT - ESB-2004.0559 -- APPLE-SA-0024-09-07 -- Security Update 2003-09-07	af854a3a-2127-422b-91ae-364da2661108	w
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	e
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

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