CVE-2004-2643

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

Summary

CVE	CVE-2004-2643
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	Directory traversal vulnerability in Microsoft cabarc allows remote attackers to overwrite files via "../" sequences in file name

Risk And Classification

Primary CVSS: v2.0 3.7 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Cabarc	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
archives.neohapsis.com/archives/fulldisclosure/2004-10/0341.html
www.osvdb.org/10714
'Microsoft cabarc directory traversal' - MARC
Files ≈ Packet Storm
IBM X-Force Exchange
Microsoft CABARC Directory Traversal Vulnerability
SecurityTracker.com Archives - Microsoft Cabarc Directory Traversal Flaw Lets Remote Users Create/Overwrite Files on the Target System
Secunia - Advisories - Cabinet Tool "Cabarc.exe" Directory Traversal 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.