CVE-2006-6134

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

Summary

CVE	CVE-2006-6134
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-11-28 01:07:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Heap-based buffer overflow in the WMCheckURLScheme function in WMVCORE.DLL in Microsoft Windows Media Player

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	Microsoft	Windows Media Player	10.00.00.4036	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Windows Media Player ASX PlayList File Heap Overflow Vulnerability	af854a3a-2127-4
ASA-2006-274 (923689)	af854a3a-2127-4
US-CERT Technical Cyber Security Alert TA06-346A -- Microsoft Updates for Multiple Vulnerabilities	af854a3a-2127-4
CXSecurity - IDS	af854a3a-2127-4
SecurityFocus	af854a3a-2127-4
Windows Media Player ASX Playlist File Buffer Overflow May Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-4
US-CERT Vulnerability Note VU#208769	af854a3a-2127-4
Windows Media Player ASX/ASF File Parsing Vulnerabilities - Advisories - Secunia	af854a3a-2127-4
Microsoft Security Bulletin MS06-078 - Critical | Microsoft Docs	af854a3a-2127-4
Repository / Oval Repository	af854a3a-2127-4
SecurityFocus	af854a3a-2127-4
Resources | BeyondTrust	af854a3a-2127-4
SecurityFocus	af854a3a-2127-4
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-4
Welcome to the Microsoft Security Response Center Blog! : Public Proof of Concept Code for ASX File Format Isssue	af854a3a-2127-4
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.