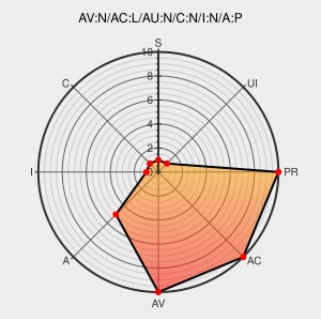
CVE-2004-1623

Published on: 10/22/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1623

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows Xp from Microsoft contain the following vulnerability:

The WAV file property handler in Windows XP SP1 allows remote attackers to cause a denial of service (infinite loop in Explorer) via a WAV file with an invalid file header whose fmt chunk length is set to 0xFFFFFFFF.

CVE-2004-1623 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 11053
'[HV-LOW] Unsafe WAV header handling can cause DoS on Windows' - MARC	marc.info text/html	BUGTRAQ 20041021 [HV-LOW] Unsafe WAV header handling can cause DoS on Windows
Microsoft Windows XP WAV File Handler Denial Of Service Vulnerability	Exploit Vendor Advisory cve.report (archive) text/html	BID 11503
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF windowsxp-explorer-wav-dos(17864)
SecurityTracker.com Archives - Microsoft Windows XP Error in	securitytracker.com	SECTRACK 1011880

Explorer in Processing WAV Files Lets Remote Users Deny Service	text/html	
404 Not Found	Exploit Vendor Advisory www.hexview.com text/plain Inactive Link Not Archived	MISC www.hexview.com/docs/20041021-1.txt

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Xp	All	All	embedded	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	embedded	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	All	embedded	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	embedded	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All

cpe:2.3:o:microsoft:windows_xp:*:*:embedded:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:home:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:home:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:media_center:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:gold:professional:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:embedded:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:home:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:media_center:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:embedded:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:home:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:media_center:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:gold:professional:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:embedded:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:home:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:media_center:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→