CVE-2006-0023

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

Summary

CVE	CVE-2006-0023
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-08 02:18:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Microsoft Windows XP SP1 and SP2 before August 2004, and possibly other operating systems and versions, uses insecur

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

EPSS: 0.007790000 probability, percentile 0.737040000 (date 2026-04-16)

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All

Vendor Declared Affected Products

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

References

Reference
404 Not Found
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Repository / Oval Repository
Your request has been blocked. This could be due to several reasons.
Microsoft Security Bulletin MS06-011 - Important | Microsoft Docs
US-CERT Vulnerability Note VU#953860
SecurityTracker.com Archives - Microsoft Windows Services Have Unsafe Default ACLs That Let Remote Authenticated Users Gain Elevated
Secunia - Advisories - Nortel Centrex IP Client Manager Windows Privilege Escalation
SecurityTracker.com Archives - Microsoft Windows UPnP/NetBT/SCardSvr/SSDP Services May Be Incorrectly Configured By 3rd Party Applic
SecurityFocus
1. Overview:
IBM X-Force Exchange
www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp
Repository / Oval Repository
Windows Insecure Service Permissions Privilege Escalation - Advisories - Secunia
Avaya Modular Messaging Windows Privilege Escalation Security Issues - Advisories - Secunia
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**