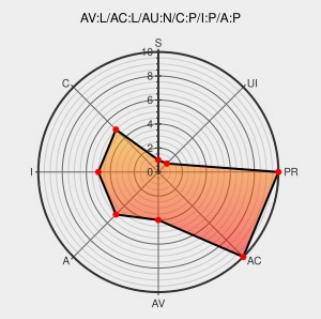
CVE-2004-2176

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2004-2176

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



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

The Internet Connection Firewall (ICF) in Microsoft Windows XP SP2 is configured by default to trust sessmgr.exe, which allows local users to use sessmgr.exe to create a local listening port that bypasses the ICF access controls.

CVE-2004-2176 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
Microsoft Windows XP Weak Default Configuration Vulnerability	Exploit, cve.report (archive), text/html	BID 11410
SecurityFocus	www.securityfocus.com, text/html	BUGTRAQ 20041012 Writing Trojans that bypass Windows XP Service Pack 2 Firewall

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	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All

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

cpe:2.3:o:microsoft:windows_xp:*:sp2:home:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp2:media_center:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:sp2:home:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp2:media_center:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→