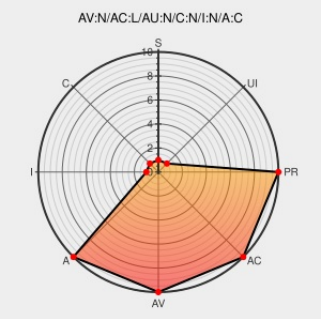
CVE-2005-3644

Published on: 11/17/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-3644

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



Certain versions of Windows 2000 from Microsoft contain the following vulnerability:

PNP_GetDeviceList (upnp_getdevicelist) in UPnP for Microsoft Windows 2000 SP4 and earlier, and possibly Windows XP SP1 and earlier, allows remote attackers to cause a denial of service (memory consumption) via a DCE RPC request that specifies a large output buffer size, a variant of CVE-2006-6296, and a different vulnerability than CVE-2005-2120.

CVE-2005-3644 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Security Webinars, Podcasts, Success Stories, White Papers, and Datasheets | eEye Digital Security	www.eeye.com text/html	MISC www.eeye.com/Resources/Security-Center/Research/Zero-Day-Tracker/2005/20051116
MS Windows 2k UPNP (getdevicelist) Memory Leak DoS Exploit	www.exploit-db.com Proof of Concept text/x-c	EXPLOIT-DB 1328
SecurityTracker.com Archives - Microsoft Windows RPC Service May Let Remote Users Deny Service	securitytracker.com text/html	SECTRACK 1015233
Microsoft Windows Plug and Play Denial of Service Vulnerability	cve.report (archive) text/html	BID 15460

Resources | BeyondTrust	research.eeye.com text/html	MISC research.eeye.com/html/alerts/zeroday/20051116.html
Félicitations ! Votre domaine a bien été créé chez OVH !	Vendor Advisory www.frsirt.com text/html	MISC www.frsirt.com/exploits/20051117.Win_upnp_getdevicelist.c.php
Your request has been blocked. This could be due to several reasons.	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MSKB 911052
SecuriTeam - Windows 2000 Server UPNP DoS (Exploit)	Exploit www.securiteam.com text/html	MISC www.securiteam.com/exploits/6V00C15EKM.html
Secunia - Advisories - Microsoft Windows UPnP GetDeviceList Denial of Service	Vendor Advisory web.archive.org text/html	SECUNIA 17595

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 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	sp1	All	All
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	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	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	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	sp2	tablet_pc	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	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	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	sp2	tablet_pc	All

cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:*:*:*:*:*:

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:home:*:*:*:*:*:

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

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:*:sp2:tablet_pc:*:*:*:*:*:

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:home:*:*:*:*:*:

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

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:*:sp2:tablet_pc:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→