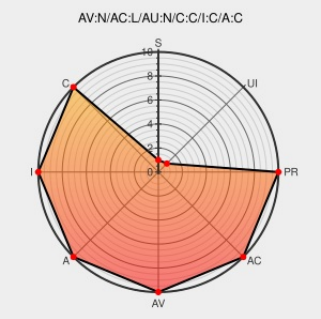
CVE-2005-1983

Published on: 08/10/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:25 PM UTC

CVE-2005-1983

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



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

Stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows 2000 and Windows XP Service Pack 1 allows remote attackers to execute arbitrary code via a crafted packet, and local users to gain privileges via a malicious application, as exploited by the Zotob (aka Mytob) worm.

CVE-2005-1983 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
Microsoft Windows Plug and Play Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 14513
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100073
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:160
404 Not Found	web.archive.org text/html Inactive Link Not Archived	MISC www.hsc.fr/ressources/presentations/null_sessions/
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-plugandplay-bo(21602)

Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:783
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:267
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:474
SecurityTracker.com Archives - Microsoft Windows Plug and Play Stack Overflow Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1014640
VU#998653 - Microsoft Plug and Play contains a buffer overflow vulnerability	US Government Resource www.kb.cert.org text/html	CERT-VN VU#998653
Microsoft Security Bulletin MS05-039 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS05-039
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-1354
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC P-266
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 18605
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:497
Neohapsis Archives - Full Disclosure List - #0384 - [Full-disclosure] Windows 2000 universal exploit for MS05-039	archives.neohapsis.com text/x-c Inactive Link Not Archived	FULLDISC 20050811 Windows 2000 universal exploit for MS05-039
Internet Security Systems -	web.archive.org text/html Inactive Link Not Archived	ISS 20050809 Windows Plug and Play Remote Compromise
SecuriTeam.com ™ - Vulnerability in Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039)	www.securiteam.com text/html	MISC www.securiteam.com/windowsntfocus/5YP0E00GKW.html
Félicitations ! Votre domaine a bien été créé chez OVH !	www.frsirt.com text/html	MISC www.frsirt.com/english/alerts/20050814.ZotobA.php
Secunia - Advisories - Microsoft Windows Plug-and-Play Service Buffer Overflow	web.archive.org text/html	SECUNIA 16372
US-CERT Technical Cyber Security Alert TA05-221A -- Microsoft Windows and Internet Explorer Vulnerabilities	Patch US Government Resource www.us-cert.gov text/html	CERT TA05-221A

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

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

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→