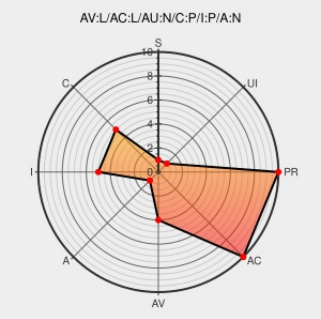
CVE-2005-1982

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

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

CVE-2005-1982

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



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

Unknown vulnerability in the PKINIT Protocol for Microsoft Windows 2000, Windows XP, and Windows Server 2003 could allow a local user to obtain information and spoof a server via a man-in-the-middle (MITM) attack between a client and a domain controller when PKINIT smart card authentication is being used.

CVE-2005-1982 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100102
US-CERT Vulnerability Note VU#477341	US Government Resource www.kb.cert.org text/html	CERT-VN VU#477341
Secunia - Advisories - Microsoft Windows Two Kerberos Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 16368
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100106

Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100096
Microsoft Windows Kerberos and PKINIT Vulnerabilities Allow Denial of Service, Information Disclosure, and Spoofing - SecurityTracker	securitytracker.com text/html	SECTRACK 1014642
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100098
Microsoft Windows Kerberos PKINIT Man In The Middle Vulnerability	cve.report (archive) text/html	BID 14520
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100100
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:100104
Microsoft Security Bulletin MS05-042 - Moderate | Microsoft Docs	docs.microsoft.com text/html	MS MS05-042

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 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	r2	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	standard	All	64-bit	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All

Operating System	Microsoft	Windows Xp	All	gold	professional	All

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

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

cpe:2.3:o:microsoft:windows_2003_server:enterprise:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:standard:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:web:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:enterprise:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:standard:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:web:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→