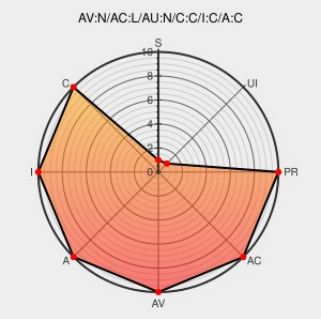
CVE-2004-0575

Published on: 10/16/2004 12:00:00 AM UTC

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

CVE-2004-0575

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



Certain versions of Windows 2003 Server from Microsoft contain the following vulnerability:

Integer overflow in DUNZIP32.DLL for Microsoft Windows XP, Windows XP 64-bit Edition, Windows Server 2003, and Windows Server 2003 64-bit Edition allows remote attackers to execute arbitrary code via compressed (zipped) folders that involve an "unchecked buffer" and improper length validation.

CVE-2004-0575 has been assigned by cve@mitre.org 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
'EEYE: Windows Shell ZIP File Decompression DUNZIP32.DLL Buffer Overflow Vulnerability' - MARC	marc.info text/html	BUGTRAQ 20041013 EEYE: Windows Shell ZIP File Decompression DUNZIP32.DLL Buffer Overflow Vulnerability
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:4276
eEye Digital Security - Vulnerability Management Solutions	www.eeye.com text/html	MISC www.eeye.com/html/research/advisories/AD20041012A.html
US-CERT Vulnerability Note VU#649374	US Government Resource www.kb.cert.org text/html	CERT-VN VU#649374
Repository / Oval Repository	oval.cisecurity.org	OVAL oval:org.mitre.oval:def:6397

	text/html	
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:1053
Microsoft Security Bulletin MS04-034 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS04-034
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-ms04034-patch(17659)
SecurityTracker.com Archives - Microsoft Windows Buffer Overflow in Processing Compressed Folders Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	SECTRACK 1011637
No Description Provided	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CIAC P-010
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF win-compressed-folders-bo(17624)
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:3913

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 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	gold	All	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	gold	All	All

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

cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→