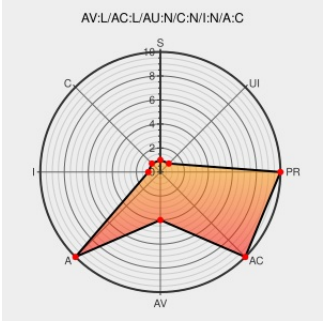
CVE-2013-3661

Published on: 05/24/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

CVE-2013-3661

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



Certain versions of Windows 7 from Microsoft contain the following vulnerability:

The EPATHOBJ::bFlatten function in win32k.sys in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012, and Windows RT does not check whether linked-list traversal is continually accessing the same list member, which allows local users to cause a denial of service (infinite traversal) via vectors that trigger a crafted PATHRECORD chain.

CVE-2013-3661 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
win32k!EPATHOBJ::pprFlattenRec Uninitialized Next Pointer Testcase	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 25611
Google engineer bashes Microsoft's handling of security researchers, discloses Windows zero-day | Computerworld	www.computerworld.com text/html	MISC www.computerworld.com/s/article/9239477
Google engineer publicizes Windows zero-day bug, claims Microsoft is 'difficult to work with' |	www.theverge.com text/html	MISC www.theverge.com/2013/5/23/4358400/google-engineer-bashes-n discloses-windows-flaw

The Verge		
Security Advisory SA53435 - Microsoft Windows Kernel Multiple Vulnerabilities - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 53435
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 93539
Tavis Ormandy na Twitterze: "I just realised a really cute trick to exploit the EPATHOBJ bug, make the list cycle, then a thread can clean up the pool, and patch it!"	nitter.domain.glass text/html	MISC twitter.com/taviso/statuses/335557286657400832
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20130603 Re: exploitation ideas under memory pressure
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20130517 Re: exploitation ideas under memory pressure
0day: Windows Kernel EPATHOBJ Vulnerability : netsec	www.reddit.com text/html	MISC www.reddit.com/r/netsec/comments/1eqh66/0day_windows_kernel_epathob

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 7	-	sp1	x64	All
Operating System	Microsoft	Windows 7	-	sp1	x86	All
Operating System	Microsoft	Windows 7	-	sp1	x64	All
Operating System	Microsoft	Windows 7	-	sp1	x86	All
Operating System	Microsoft	Windows 8	-	-	x64	All
Operating System	Microsoft	Windows 8	-	-	x86	All
Operating System	Microsoft	Windows 8	-	-	x64	All
Operating System	Microsoft	Windows 8	-	-	x86	All
Operating System	Microsoft	Windows Rt	-	All	All	All

System						
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All

cpe:2.3:o:microsoft:windows_7:-:sp1:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:-:sp1:x86:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:-:sp1:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_7:-:sp1:x86:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_8:-:-:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_8:-:-:x86:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_8:-:-:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_8:-:-:x86:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_rt:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_rt:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:-:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:-:sp2:x64:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→