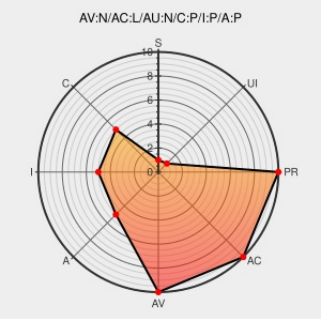
CVE-2013-2556

Published on: 03/11/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:41 PM UTC

CVE-2013-2556

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



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

Unspecified vulnerability in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 through SP1 allows attackers to bypass the ASLR protection mechanism via unknown vectors, as demonstrated against Adobe Flash Player by VUPEN during a Pwn2Own competition at CanSecWest 2013, aka "ASLR Security Feature Bypass Vulnerability."

CVE-2013-2556 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Microsoft Updates for Multiple Vulnerabilities | US-CERT	US Government Resource, www.us-cert.gov, text/html	CERT TA13-225A
Pwn2Own 2013 - HP Enterprise Business Community	web.archive.org, text/html, Inactive Link, Not Archived	MISC h30499.www3.hp.com/t5/HP-Security-Research-Blog/Pwn2Own-2013/ba-p/5981157
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:18132
JavaScript is not available.	nitter.domain.glass, text/html	MISC twitter.com/VUPEN/statuses/309713355466227713

Zero Day Initiative na Twitterze: "@VUPEN just took down Adobe Flash for $70k and a grand total of $250k! #pwn2own"	nitter.domain.glass text/html	MISC twitter.com/thezdi/statuses/309756927301283840
Microsoft Security Bulletin MS13-063 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS13-063

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 Server 2008	All	r2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	r2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Server 2008	All	r2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	r2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All

System						
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	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_server_2008:*:r2:itanium:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:r2:x64:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:sp2:itanium:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x64:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x86:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:r2:itanium:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:r2:x64:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:sp2:itanium:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x64:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_server_2008:*:sp2:x86:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report