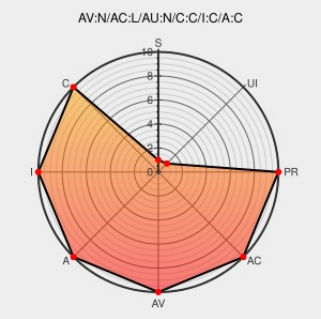
CVE-2004-2289

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2289

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



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

Microsoft Windows XP Explorer allows local users to execute arbitrary code via a system folder with a Desktop.ini file containing a .ShellClassInfo specifier with a CLSID value that is associated with an executable file.

CVE-2004-2289 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
Winxp executing folder	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	MISC www.freewebs.com/roozbeh_afrasiabi/xploit/execute.htm
Microsoft Windows XP Self-Executing Folder Vulnerability	cve.report (archive), text/html	BID 10363
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF winxp-explorer-code-execution(16171)
Neohapsis Archives - Bugtraq - #0168 - Desktop.ini flaw results in executing folders	Exploit, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20040517 Desktop.ini flaw results in executing folders

Secunia - Advisories - Microsoft Windows "desktop.ini" Arbitrary File Execution Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 11633
Microsoft Security Bulletin MS06-015 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS06-015
No Description Provided	Exploit www.osvdb.org Inactive Link Not Archived	OSVDB 6221

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 Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All

cpe:2.3:o:microsoft:windows_xp:*:*:home:*:*:*:*:*:

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

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

cpe:2.3:o:microsoft:windows_xp:*:*:home:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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