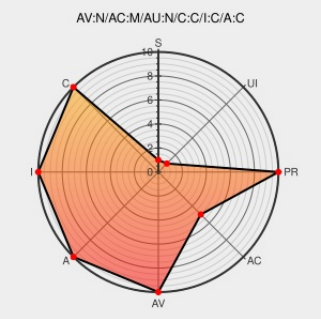
CVE-2010-3144

Published on: 08/27/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:04 PM UTC

CVE-2010-3144

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



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

Untrusted search path vulnerability in the Internet Connection Signup Wizard in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 allows local users to gain privileges via a Trojan horse smmscrpt.dll file in the current working directory, as demonstrated by a directory that contains an ISP or INS file, aka "Internet Connection Signup Wizard Insecure Library Loading Vulnerability."

CVE-2010-3144 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Microsoft Windows Internet Connection Signup Wizard May Load DLLs Unsafely and Remotely Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1024879
US-CERT Technical Cyber Security Alert TA10-348A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/xml	CERT TA10-348A
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11993
Microsoft Security Bulletin MS10-097 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS10-097
Microsoft Internet Connection Signup Wizard DLL Hijacking Exploit (smmscrpt.dll)	Exploit	EXPLOIT-DB 14754

www.exploit-db.com
Proof of Concept
text/html

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 Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	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_server_2003:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_server_2003:*: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→

site. This site includes MITRE data granted under the following license.

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