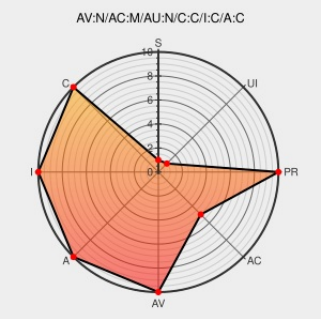
CVE-2010-3145

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

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

CVE-2010-3145

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



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

Untrusted search path vulnerability in the BitLocker Drive Encryption API, as used in sdclt.exe in Backup Manager in Microsoft Windows Vista SP1 and SP2, allows local users to gain privileges via a Trojan horse fveapi.dll file in the current working directory, as demonstrated by a directory that contains a Windows Backup Catalog (.wbcat) file, aka "Backup Manager Insecure Library Loading Vulnerability."

CVE-2010-3145 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
US-CERT Technical Cyber Security Alert TA11-011A -- Microsoft Updates for Multiple Vulnerabilities	US Government Resource, www.us-cert.gov, text/xml	CERT TA11-011A
Microsoft Security Bulletin MS11-001 - Important | Microsoft Docs	docs.microsoft.com, text/html	MS MS11-001
Microsoft Vista BitLocker Drive Encryption API Hijacking Exploit (fveapi.dll)	Exploit, www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 14751
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:12273

Webmail - OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2011-0074
Windows Backup Manager May Load DLLs Unsafely and Remotely Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1024948

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 Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	All	sp1	All	All
Operating System	Microsoft	Windows Vista	All	sp1	x64	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All

cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp1:x64:*:*:*:*:*:

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

cpe:2.3:o:microsoft:windows_vista:*:sp2:x64:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp1:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_vista:*:sp1: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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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