



CVE-2008-2511

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2008-2511
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-02 21:30:00 UTC
Updated	2018-10-11 20:41:00 UTC
Description	Directory traversal vulnerability in the UmxEventCli.CachedAuditDataList.1 (aka UmxEventCliLib) ActiveX control in UmxEv

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ca	Internet Security Suite Plus 2008	All	All	All	All
Application	Ca	Internet Security Suite Plus 2008	All	All	All	All

References

Reference	Source
IBM X-Force Exchange	XF
CA Internet Security Suite Multiple ActiveX Controls Insecure Methods - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECU
SecurityFocus	BUGT
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPE
CA Internet Security 'UmxEventCliLib' ActiveX Control Lets Remote Users Corrupt Files - SecurityTracker	SECT
Error 404 :(MISC
CA Internet Security Suite 2008 - 'SaveToFile()' File Corruption (PoC) - Windows dos Exploit	EXPL
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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 registered 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](#)