CVE-2008-2463

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-2463
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-07-07 23:41:00 UTC
Updated	2017-09-29 01:31:00 UTC
Description	The Microsoft Office Snapshot Viewer ActiveX control in snapview.ocx 10.0.5529.0, as distributed in the standalone Snapsh

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office Snapshot Viewer Activex	office2000	All	All	All
Application	Microsoft	Office Snapshot Viewer Activex	office_2003	All	All	All
Application	Microsoft	Office Snapshot Viewer Activex	office_xp	All	All	All
Application	Microsoft	Office Snapshot Viewer Activex	office2000	All	All	All
Application	Microsoft	Office Snapshot Viewer Activex	office_2003	All	All	All
Application	Microsoft	Office Snapshot Viewer Activex	office_xp	All	All	All

References

Reference
VU#837785 - Microsoft Office Snapshot Viewer ActiveX control race condition
Microsoft Access (Snapview.ocx 10.0.5529.0) ActiveX Remote Exploit
SecurityTracker.com Archives - Microsoft Access Snapshot Viewer ActiveX Control Lets Remote Users Download Files to Arbitrary Locations
IBM X-Force Exchange
US-CERT Technical Cyber Security Alert TA08-225A -- Microsoft Updates for Multiple Vulnerabilities
Repository / Oval Repository
US-CERT Technical Cyber Security Alert TA08-189A -- Microsoft Office Snapshot Viewer ActiveX Vulnerability
Microsoft Access Snapshot Viewer ActiveX Control Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download Vulnerability
HPSBST02360
Your request has been blocked. This could be due to several reasons.
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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