



CVE-2006-2273

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

Summary

CVE	CVE-2006-2273
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-05-12 00:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The InstallProduct routine in the Verisign VUpdater.Install (aka i-Nav) ActiveX control does not verify Microsoft Cabinet (.CAB) files, which could allow an attacker to execute arbitrary code on a system.

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

EPSS: 0.042370000 probability, percentile 0.887970000 (date 2026-04-17)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Verisign	I-nav	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
IBM X-Force Exchange				af854a3a-2127-422b-91a6		
Verisign i-Nav ActiveX Control Remote Buffer Overflow Vulnerability				af854a3a-2127-422b-91a6		
VeriSign i-Nav ActiveX Plugin CAB Validation Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker				af854a3a-2127-422b-91a6		
SecurityFocus				af854a3a-2127-422b-91a6		
SecurityReason				af854a3a-2127-422b-91a6		
www.osvdb.org/25431				af854a3a-2127-422b-91a6		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-2127-422b-91a6		
ZDI-06-014 Zero Day Initiative				af854a3a-2127-422b-91a6		
Verisign i-NAV ActiveX Control Arbitrary Code Execution - Advisories - Secunia				af854a3a-2127-422b-91a6		
CVE Program record				CVE.ORG		
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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)