



CVE-2007-4034

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

Summary

CVE	CVE-2007-4034
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-27 22:30:00 UTC
Updated	2011-03-07 05:00:00 UTC
Description	Stack-based buffer overflow in the YDPCTL.YDPControl.1 (aka Yahoo! Installer Plugin for Widgets) ActiveX control before 1.0.0.0

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yahoo	Widgets	All	All	All	All

References

Reference	Source
Yahoo! Widgets Engine YDPCTL.DLL ActiveX Control Buffer Overflow Vulnerability	BID
37705	OSVDB
VU#120760 - Yahoo! Installer Plugin for Widgets ActiveX control stack buffer overflow	CERT-VN
About the July 24, 2007 Widgets Security Updates - Yahoo! Widgets	CONFIRM
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Yahoo! Widgets Buffer Overflow in 'YDPCTL.dll' ActiveX Control Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK
Yahoo! Widgets YDP ActiveX Control Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA
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](#)