

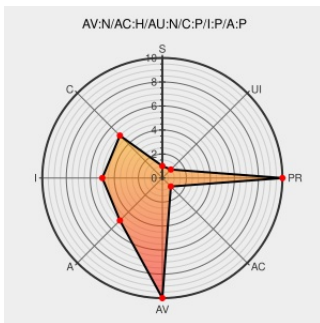


CVE-1999-1575

Published on: 09/10/1999 04:00:00 AM UTC

Last Modified on: 07/22/2021 02:02:00 PM UTC

CVE-1999-1575

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of **ie** from **Microsoft** contain the following vulnerability:

The Kodak/Wang (1) Image Edit (imgedit.ocx), (2) Image Annotation (imgedit.ocx), (3) Image Scan (imgscan.ocx), (4) Thumbnail Image (imgthumb.ocx), (5) Image Admin (imgadmin.ocx), (6) HHOOpen (hhopen.ocx), (7) Registration Wizard (regwizc.dll), and (8) IE Active Setup (setupctl.dll) ActiveX controls for Internet Explorer (IE) 4.01 and 5.0 are marked as "Safe for Scripting," which allows remote attackers to create and modify files and execute arbitrary commands.

CVE-1999-1575 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.1 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CERT/CC Vulnerability Note VU#41408	US Government Resource www.kb.cert.org text/html	CERT-VN VU#41408
CERT/CC Vulnerability Note VU#23412	US Government Resource www.kb.cert.org text/html	CERT-VN VU#23412
Microsoft Security Bulletin MS99-037 - Critical Microsoft Docs	docs.microsoft.com text/html	MS MS99-037
CERT/CC Vulnerability Note VU#9162	US Government Resource www.kb.cert.org text/html	CERT-VN VU#9162

SecurityFocus home mailing list: BugTraq	Exploit www.securityfocus.com text/html	BUGTRAQ 19990924 Several ActiveX Buffer Overruns
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF wang-kodak-activex-control(7097)
CERT/CC Vulnerability Note VU#26924	US Government Resource www.kb.cert.org text/html	CERT-VN VU#26924
CERT/CC Vulnerability Note VU#24839	US Government Resource www.kb.cert.org text/html	CERT-VN VU#24839

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
Application	Microsoft	Ie	4.0.1	All	All	All
Application	Microsoft	Ie	5.0	All	All	All
Application	Microsoft	Ie	4.0.1	All	All	All
Application	Microsoft	Ie	5.0	All	All	All
Application	Microsoft	Internet Explorer	4.0.1	All	All	All
Application	Microsoft	Internet Explorer	5.0	All	All	All
cpe:2.3:a:microsoft:ie:4.0.1:*:*:*:*:*:						
cpe:2.3:a:microsoft:ie:5.0:*:*:*:*:*:						
cpe:2.3:a:microsoft:ie:4.0.1:*:*:*:*:*:						
cpe:2.3:a:microsoft:ie:5.0:*:*:*:*:*:						
cpe:2.3:a:microsoft:internet_explorer:4.0.1:*:*:*:*:*:						
cpe:2.3:a:microsoft:internet_explorer:5.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)