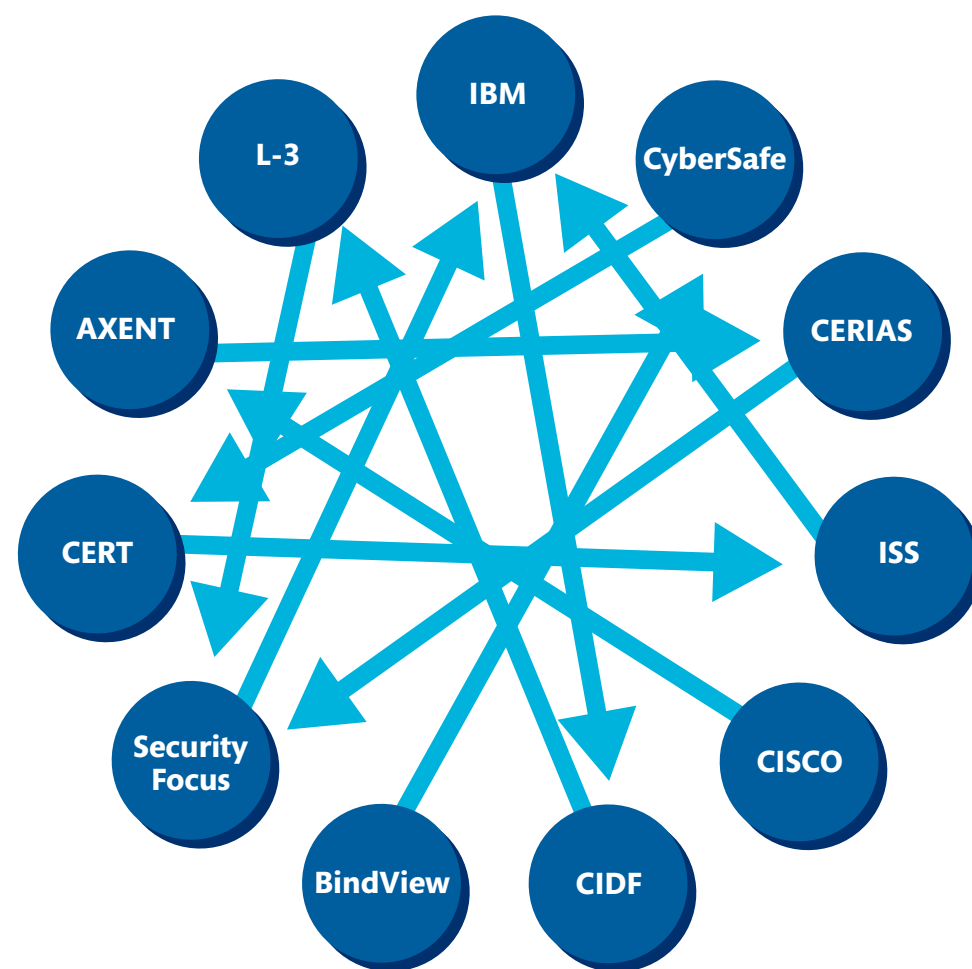


cve.mitre.org



A central yellow circle labeled "CVE" is surrounded by twelve blue circles, each containing the name of an organization. Light blue arrows point from each of these outer circles toward the central "CVE" circle, indicating their contribution to the program. The organizations are: IBM, CyberSafe, CERIAS, ISS, CISCO, CIDEF, BindView, Security Focus, CERT, AXENT, L-3, and IBM.

- CVE is the standard for information security vulnerability names
- CVE lists over 55,000 unique identifiers
- CVE is used in over 130 products by over 75 vendors
- There are more than 20 CVE Numbering Authorities (CNAs)

CVE LIST
COMPATIBILITY
NEWS — FEBRUARY 7, 2013
SEARCH

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

HOME > CVE > CVE-2011-5046

About CVE

- Terminology
- Documents
- FAQs

CVE List

- About CVE Identifiers
- Search CVE
- Search NVD
- Updates & RSS Feeds
- Request a CVE-ID

CVE In Use

- CVE-Compatible Products
- NVD for CVE Fix Information
- CVE Numbering Authorities

News & Events

- Calendar
- Free Newsletter

Community

- CVE Editorial Board
- Sponsor
- Contact Us

Search the Site

- Site Map

TOTAL CVEs: 54586

1. Flat Identifier

CVE-ID

CVE-2011-5046

[Learn more at National Vulnerability Database \(NVD\)](#)

- Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The Graphics Device Interface (GDI) in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate user-mode input, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted data, as demonstrated by a large height attribute of an IFRAME element rendered by Safari, aka "GDI Access Violation Vulnerability."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:18275
- URL:<http://www.exploit-db.com/exploits/18275>
- MISC:<http://twitter.com/w3bd3vil/statuses/148454992989261824>
- MS:MS12-008
- URL:<http://technet.microsoft.com/security/bulletin/MS12-008>
- OSVDB:77908
- URL:<http://osvdb.org/77908>
- OVAL:oval.org.mitre.oval:def:14603
- URL:<http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:14603>
- SECTRAK:1026450
- URL:<http://www.securitytracker.com/id?1026450>
- SECUNIA:47237
- URL:<http://secunia.com/advisories/47237>
- XF:ms-win32k-iframe-code-exec(71873)
- URL:<http://xforce.iss.net/xforce/xfdb/71873>

Date Entry Created

20111230	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
-----------------	--

Phase (Legacy)

Assigned (20111230)

CVE List

- About CVE Identifiers
- Editorial Policies
- Data Sources
- Reference Key/Maps
- Search Tips
- Updates & RSS Feeds
- Request a CVE Identifier

ITEMS OF INTEREST

- Terminology
- NVD

2. Short Description

External
References