CVE-2004-0566

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

Summary

CVE	CVE-2004-0566
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-07-27 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Integer overflow in imgbmp.cxx for Windows 2000 allows remote attackers to execute arbitrary code via a BMP image with

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Internet Explorer	5.0	All	All	All

Application	Microsoft	Internet Explorer	5.0.1	All	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp1	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp2	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp3	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp4	All	All
Application	Microsoft	Internet Explorer	5.5	All	All	All
Application	Microsoft	Internet Explorer	5.5	sp1	All	All
Application	Microsoft	Internet Explorer	5.5	sp2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sou
Neohapsis Archives - Full Disclosure List - #0806 - [Full-Disclosure] GAYER THAN AIDS ADVISORY #01: IE 5 remote code execution	af85
Repository / Oval Repository	af85
IBM X-Force Exchange	af85
Repository / Oval Repository	af85
Microsoft Security Bulletin MS04-025 - Critical | Microsoft Docs	af85
Repository / Oval Repository	af85
Repository / Oval Repository	af85
US-CERT Vulnerability Note VU#266926	af85
US-CERT Technical Cyber Security Alert TA04-212A -- Critical Vulnerabilities in Microsoft Windows	af85
Repository / Oval Repository	af85
CVE Program record	CVE
NVD vulnerability detail	NVD

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**